

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-243707

(43)Date of publication of application : 07.09.2001

-----  
(51)Int.Cl. G11B 20/10

G06F 1/26

G06F 12/14

-----  
(21)Application number : 2000-054129 (71)Applicant : SONY CORP

(22)Date of filing : 29.02.2000 (72)Inventor : HOSOGAYA NORIBUMI

-----  
(54) INFORMATION TRANSMISSION AND RECEPTION SYSTEM AND  
ELECTRONIC EQUIPMENT

(57)Abstract:

PROBLEM TO BE SOLVED: To obtain diversity concerning restrictions on operations for the copyright protection in a system.

SOLUTION: In an information transmission and reception system in which a personal computer and a portable audio player are connected with a USB cable, data whose copyrights should be protected, such as audio data, are transmitted and received by copying or transferring them and power is supplied from the personal computer to the portable audio player, mutual authentication is performed between two pieces of equipment. According to an authentication result, the power supplied through the USB cable is controlled.

**\* NOTICES \***

**JPO and INPIT are not responsible for any damages caused by the use of this translation.**

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

---

**CLAIMS**

---

[Claim(s)]

[Claim 1]Have the 2nd electronic equipment characterized by comprising the following, and while, A mutual recognition processing means to perform mutual recognition processing about the 1st electronic equipment and the 2nd electronic equipment which are connected by the 1st connecting means of the above, and the 2nd connecting means of the above, An information transmission and reception system having a power control means which controls current supply to an internal circuit of the 1st electronic equipment of the above to the 2nd electronic equipment of the above according to an authentication result of the above-mentioned mutual recognition processing.

The 1st memory measure made memorizable [ two or more contents information ].  
Transmission and reception of information on connected external electronic

equipment.

The 1st connecting means in which current supply to connected external electronic equipment is possible.

The 1st electronic equipment it has, and two or more contents information by the 2nd memory measure made memorizable and being connected with the 1st electronic equipment of the above. Transmission and reception of information including the above-mentioned contents information between the 1st electronic equipment of the above and a power supply supplied from the 1st electronic equipment of the above are inputted, and it is the 2nd connecting means that can be supplied to an internal circuit.

[Claim 2]Electronic equipment comprising:

A memory measure made memorizable [ two or more contents information ].

Transmission and reception of information on connected external electronic equipment.

A connecting means in which current supply to connected external electronic equipment is possible.

A power control means which controls current supply to external electronic equipment according to a mutual recognition processing means to perform mutual recognition processing, and an authentication result of the above-mentioned mutual recognition processing, about external electronic equipment connected by the above-mentioned connecting means.

[Claim 3]Electronic equipment comprising:

A memory measure made memorizable [ two or more contents information ].

Transmission and reception of information on connected external electronic equipment.

A power supply supplied from connected external electronic equipment is inputted, and it is a connecting means which can be supplied to an internal circuit.

A power control means which controls supply to an internal circuit of a power supply supplied from the above-mentioned external electronic equipment according to a mutual recognition processing means to perform mutual recognition processing, and an authentication result of the above-mentioned mutual recognition processing, about external electronic equipment connected by the above-mentioned connecting means.

2.\*\*\*\* shows the word which can not be translated.

3.In the drawings, any words are not translated.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to the information transmission and reception system which comprises electronic equipment which transmits and receives contents information, such as audio information, for example, and the electronic equipment which constitutes this information transmission and reception system.

[0002]

[Description of the Prior Art]As a usage pattern of the personal computer in recent years, save as a file the audio information played, for example from CD (Compact Disc) or other recording media at storages, such as a hard disk, or, Or downloading audio information from the site of the Internet, etc. and saving this as a file at a hard disk is performed.

[0003]By thus, the thing for which an inside is equipped with recording media, such as a flash memory, for example as an audio player which can use the file of the audio information saved at the hard disk of the personal computer. The portable audio player with which the large miniaturization was attained is also spreading.

[0004]In using the above-mentioned portable audio player, For example, a user connects a personal computer and a portable audio player via a predetermined data

bus, transmits the audio file saved at the hard disk of the personal computer, and writes in and records on the flash memory of a portable audio player. And the audio information recorded on the flash memory by the portable audio player side is reproduced, headphone etc. are connected and this is heard.

[0005]

[Problem(s) to be Solved by the Invention]By the way, in the system which comprises a personal computer which was described above, for example, and a portable audio player, data transfer, such as a copy of data (duplicate) and movement, will be performed between recording media. Therefore, in a certain grade, a data transfer needs to be made to be restricted when it sees from a viewpoint of copyright protection. That is, if data transfer is permitted indefinitely, a possibility of infringing on copyright will come out. In order that a general user can enjoy the above using forms on the other hand, it is not appropriate to forbid data transfer thoroughly. Therefore, though copyright protection is planned, it is called for that it is made to be carried out in the data transfer management with the pliability of a certain grade whose duplicate of the data of the grade which is in a user's private use area and is accepted is enabled.

[0006]

[Means for Solving the Problem]Then, this invention is constituted as follows in consideration of the above-mentioned technical problem. First, the 1st memory measure whose memory of two or more contents information is enabled as an information transmission and reception system, The 1st electronic equipment provided with the 1st connecting means in which transmission and reception of information on connected external electronic equipment and current supply to connected external electronic equipment are possible, The 2nd memory measure made memorizable [ two or more contents information ], The 2nd electronic equipment that inputs a power supply supplied from transmission and reception and the 1st electronic equipment of information which include contents information between the 1st electronic equipment by being connected with the 1st electronic equipment, and is provided with the 2nd connecting means that can be supplied to an internal circuit shall be comprised. And a mutual recognition processing means to perform mutual recognition processing about the 1st electronic equipment and the 2nd electronic equipment which are connected by the 1st connecting means and 2nd connecting means, We decided to have a power control means which controls current supply to an internal circuit of the 1st electronic equipment to the 2nd electronic equipment according to an authentication result of mutual recognition processing.

[0007]Transmission and reception of information on a memory measure made memorizable [ two or more contents information ] and connected external electronic equipment, A connecting means in which current supply to connected external electronic equipment is possible, and a mutual recognition processing means to perform mutual recognition processing about external electronic equipment connected by this connecting means, We decided to have a power control means which controls current supply to external electronic equipment according to an authentication result of account mutual recognition processing, and to constitute electronic equipment.

[0008]Transmission and reception of information on a memory measure made memorizable [ two or more contents information ] and connected external electronic equipment, Input a power supply supplied from connected external electronic equipment, and A connecting means which can be supplied to an internal circuit, We decided to have a mutual recognition processing means to perform mutual recognition processing about external electronic equipment connected by this connecting means, and a power control means which controls supply to an internal circuit of a power supply supplied from external electronic equipment according to an authentication result of mutual recognition processing, and to constitute electronic equipment.

[0009]According to each above-mentioned composition, two electronic equipment by connecting by a mutual connecting means. An information transmission and reception system that transmission and reception of contents information and current supply from one electronic equipment to electronic equipment of another side are performed is constituted, and mutual recognition which judges whether mutual electronic equipment is based on a transceiver standard of contents information, for example is performed in transmission and reception of information. And while described above, according to an authentication result, it is constituted so that current supply from electronic equipment to electronic equipment of another side may be controlled, but it becomes possible for power control to restrict operation of electronic equipment which is not attested by this, for example.

[0010]

[Embodiment of the Invention]Hereafter, carrying of operation of this invention is explained. Subsequent explanation is given in the following order.

1. Usage pattern 1-3. internal configuration 5. data transfer processing 5-1. check-out processing 5-2. check-in processing 6. mutual recognition processing and source control processing of information transmission and reception system 1-1. entire configuration 1-2. system [0011]1. Information transmission and reception

system 1-1. entire configuration drawing 1 shows the entire configuration of the information transmission and reception system as an embodiment of the invention in outline. As an information transmission and reception system of this embodiment, the personal computer 10 which a user owns, for example, and the portable audio player (it is also only henceforth called a player) 20 are comprised.

[0012]In this case, the personal computer 10 is used as apparatus for acquiring the contents data as a musical piece which should be transmitted to the player 20, for example, saving as a file to storage devices, such as a hard disk. And in acquisition of contents data, the following two methods are mentioned greatly.

[0013]The audio information incorporated via the voice input/output interface with which the personal computer 10 is equipped although not illustrated to one here, The audio information played from the disk medium of CD format with the CD-ROM drive etc. is acquired as contents data.

[0014]One is the method of downloading and acquiring the contents data as a musical piece distributed via a network. For example, the EMD (Electrical Music Distribution) server 1 and communication of the personal computer 10 are enabled via networks, such as the Internet. Much contents data for distribution is stored in EMD server 1. Let contents data here be the audio information as a musical piece. And the user of the personal computer 10 chooses the contents data as a musical piece which should be purchased by operation to the personal computer 10, for example. And determination of the contents data to purchase will require distribution of this contents data from EMD server 1 in the personal computer 10. In EMD server 1, the transmission output of the contents data of a musical piece according to this demand is carried out to the personal computer 10. Contents data is received and saved in the personal computer 10.

[0015]As the personal computer 10 of this embodiment, It has a copyright protection function for planning copyright protection at the time of delivering and receiving contents data between the personal computer 10 and a player, as it mentions later besides [ which acquires contents data as mentioned above and saves a file ] a function. As a copyright protection function, an enciphering function, the authenticating processing function at the time of contents data transmission and reception, etc. are given, for example. And such a function is obtained by installing in the personal computer 10 the application software (henceforth "contents managing application") for managing the contents data which the manufacturing maker of the player 20 provides, for example. The above-mentioned contents managing application and the contents data in which the player 20 of this embodiment corresponds, It is

considered as the audio information by which compression processing was carried out with the method called ATRAC3 which improved the ATRAC (Adaptive Transform Acoustic Coding) method. As an embodiment, it does not need to be limited to this compression technology. As one of the data interfaces with peripheral equipment, USB (Universal Serial Bus) is provided in the personal computer 10, and the player 20 explained below is connected to it so that communication by USB is possible. [0016]The player 20 is an audio player which can reproduce and hear contents data, while it has portable size shape and a user carries, considers it as the media which carry out record reproduction of the contents data as a musical piece, and builds in the flash memory.

[0017]By the headset jack 22 being formed in the upper part flat-surface part of the main part 21 of the player 20, inserting the headphone plug 41 of the headphone 40 to here, and equipping an ear with IYADORAIBA 42. The user can hear the reproduced contents data as a sound. The manual operation button 23 of cylindrical shape is formed in the same upper part flat-surface part of the main part 21. This manual operation button 23 is performing predetermined pressing operation and rotatably operating, and is made possible [ reproduction/halt of contents data, search, a rapid traverse / already operating return etc. ]. The volume key 24, the low-pitched sound / volume restriction key 25, and the hold key 26 are formed in the lateral portion of the main part 21. The volume key 24 adjusts the audio loudness level of sound which can be heard by the headphone 40, and low-pitched sound / volume restriction key 25 is performing prescribed operation, and it performs level adjustment of a low-pitched sound region, and ON-and-OFF setting out of the function to restrict the maximum volume to a certain predetermined level. The hold key 26 is used to repeal operation to the handler provided in the player 20. It is the public places in a train etc., for example, the volume restriction key 25 is used, when a sound leaks to the circumference and it makes it like to make trouble to it, and a hold key is used for it to prevent performing operation to the operation key of a main part carelessly.

[0018]In the field used as the transverse plane of the main part 21 side, the indicator 30, the play mode key 27, and the De Dis play key 28 are formed. The predetermined display according to the operation situation of the player 20 is performed in the indicator 30. For example, during reproduction, the present operating state, a tune number, lapsed time, etc. are displayed. When the display information in this indicator 30 can be changed, for example, the De Dis play key 28 is operated by operating the De Dis play key 28, It is supposed that it is possible to switch to the state of displaying a track name, an artist name, etc., from the state which shows a tune number and

lapsed time, or to switch to the state of displaying the bit rate of the bar display and contents data in which a regenerative signal level is shown in spectrum analyzer. The play mode key 27, for example One music repeat reproduction, all-songs repeat reproduction, It is provided in order to set up special reproduction modes, such as shuffle reproduction, and the special reproduction mode set up by this key operation is also shown by the predetermined display style by the segment display in the indicator 30, for example.

[0019]USB connector 32 is formed in the lateral portion bottom of the main part 21 in which the volume key 24 grade is provided. So that it may be provided in order to connect this USB connector 32 with the personal computer 10 with USB cable 50 so that communication is possible, for example, it may illustrate, One USB plug 52 of USB cable 50 is connected with USB connector 32 of the player 20, and it is made to be connected to the USB connector (here, not shown) in which the USB plug 51 of another side is formed at the personal computer 10 side. Thus, by being connected, data transmission and reception is performed between the personal computer 10 and the player 20, and it becomes possible to deliver and receive contents data of each other. When not connecting the USB plug 52 to USB connector 32, USB connector 32 is covered by the connector covering device 33, and it can protect.

[0020]1-2. the usage pattern of a system -- here, explain the example of a usage pattern of the above-mentioned system. As it is shown in drawing 2 (a), a certain contents data CT is purchased and downloaded, and it is made to be incorporated from EMD server 1 in the personal computer 10. Thus, acquired contents data CT is changed into the file to which compression processing was performed as it mentioned above in the personal computer 10, and encryption was given, for example, is saved at an internal hard disk. Here, although not illustrated, as stated also in advance, the audio information obtained from media and voice input/output interfaces, such as CD, can also be acquired as contents data, and can be saved.

[0021]And as contents data CT saved with the personal computer 10 as mentioned above is shown in drawing 2 (b), it is made possible [ uploading to the player 20 connected via the USB interface ]. In the player 20, this uploaded contents data is written in a built-in flash memory, and is memorized. And the user can reproduce and hear the audio information which is a musical piece as contents memorized by the flash memory by the player 20.

[0022]It is supposed that the system of this embodiment is based on the copyright protection standard of SDMI (Secure Digital Music Initiative). That is, the contents managing application installed in the personal computer 10 and the player 20 are

constituted so that operation based on this SDMI may be obtained.

[0023]Drawing 3 shows the typical data transfer restrictions based on this SDMI. Here, about transmitting it from the personal computer 10, to the player 20, as contents data is copied, it is called "check-out." The data transfer in this case is a copy, and the contents data of a copied material will remain in the personal computer 10, without being deleted. It is called check-in to transmit data from the player 20 to the personal computer 10 conversely. However, the contents data which became with movement of data in check-in, therefore was memorized by the player 20 side depending on check-in is deleted.

[0024]Here, it shall be decided by check-out that it is to 3 times, and four check-out or more shall not be performed. That is, from the personal computer 10, to other apparatus containing the player 20 of this embodiment, it is restricted so that it can copy only to 3 times. However, if you check in at the contents data in which he was already checked out 3 times, for example, it will enable it to be again checked out about this contents data at which he checked in. the upload to the compression processing, the encryption processing, and the player 20 to download of the contents data from EMD server 1, and download data which were stated by drawing 2 and drawing 3 when stated for the check -- and, The contents managing application installed in the personal computer 10 performs the above-mentioned management of check-in/check-out.

[0025]By the way, providing contents data "with reproduction restrictions" is also performed. [ which provided restriction of a refreshable period or the number of times of refreshable for the purpose of being reflected / intention / giving diversity to distribution service, for example, / an owner of a copyright / as data distribution in EMD server 1 ] These refreshable periods and number of times of refreshable are stored as reproduction condition data, for example in the header of contents data.

[0026]As this embodiment, about such contents data with reproduction restrictions. Only reproduction by starting contents managing application on the personal computer 10 is enabled, and the check-out to the player 20 is managed as what cannot be performed.

[0027]However, contents data with reproduction restrictions is able to check out contents data CT with reproduction restrictions to the player 20, and to constitute by the player 20, of course, so that it may be refreshable. And as a matter of course, according to the refreshable period and the number of times of refreshable specified by contents data CT with reproduction restrictions, it should be constituted so that the reproduction motion in the player 20 may also be restricted.

[0028]Then, the internal configuration of the personal computer 10 which constitutes the system shown in drawing 1, and the player 20 is explained with reference to drawing 4. It is that the network connection interface 101 for connecting with the network 2 is established in the personal computer 10, and the network connection interface 101 functions by control of CPU102, \*\* which can download the contents data which is connected with EMD server 1 via the network 2 so that communication is possible, and is provided with EMD server 1

[0029]CD-ROM drive 106 is formed here and it is supposed in this CD-ROM drive 106 that it is possible to play and read the data currently recorded on the disk in CD format with which it was loaded. For example, in addition to the disk in CD format, a disk drive also with refreshable disks, such as DVD (Digital Versatile Disc), may be formed actually. For example, the audio information which played and obtained the disk with which this CD-ROM drive 106 was loaded as contents data can be used.

[0030]The voice input/output interface 108 is considered as the interface for input and output of a digital audio signal with an external instrument, or an analog audio signal. In the personal computer 10 of this embodiment, it is also made possible to change into contents data the digital audio signal and analog audio signal which are inputted via this voice input/output interface 108.

[0031]At the hard disk 107, various application software for CPU102 to perform and various files are saved. For example, if it is a case of this embodiment, the file of the contents data which contents managing application and this contents managing application treat is saved here.

[0032]RTC105 clocks current time and outputs the time information. The current time information acquired in this RTC105 can be used for the reproduction period management of contents data, etc. in this embodiment.

[0033]The interface 10 has an user interface function for transmitting to CPU102 the operation information inputted from the operation input section 112 actually used as a mouse, a keyboard, etc., for example, and displaying a picture on the display 113. It is assumed that it also has the data interface function with external peripheral equipment. And in order communication with external peripheral equipment is possible, and to be made by the USB interface at least as this embodiment, therefore to realize the data communications by a USB interface in the interface 10, the USB driver 110 is formed. The USB driver 110 is connected with USB connector 111 actually expressed and provided, for example in personal computer 10 main part. When it was a case of this embodiment and is connected with the player 20 by the USB interface, according to the program of contents managing application, the contents data as a musical piece

can be transmitted to the player 20. That is, by control of CPU102, contents data is transmitted to the USB driver 110, and carries out the transmission output of the contents data via USB connector 111 with the USB driver 110.

[0034]As shown here also as USB cable 50 which connects USB connector 111 by the side of the personal computer 10, and USB connector 32 by the side of the player 20, As a USB interface, one cable (transmission line) is formed with signal-line D+, D-, power source line Vbus, and four lines of ground lines. Signal-line D+ and D- are lines for data which perform data communications by difference transmission, and let power source line Vbus be a line by the side of the plus for performing current supply from the personal computer 10. That is, with the USB interface, it is supposed as everyone knows that it is possible to perform DC-power-supply supply, for example from the personal computer 10 to peripheral equipment.

[0035]CPU(Central Processing Unit) 102, In the personal computer 10, necessary control management is performed according to the program as an OS (Operation System), and the started program of various application software. ROM113 is used as nonvolatile memory, such as EEPROM and a flash memory, for example, and is made possible [ saving suitably the data of various setup information the file which does not have the data volume like \*\*, etc. ]. The program data of application software started, for example and the various data obtained by processing of CPU12 are held RAM104.

[0036]The power supply section 114 inputs commercial alternating current power actually, for example, and gets the DC power supply voltage of a predetermined level. And the power supply PW acquired by doing in this way is supplied to each internal functional circuit unit. As it mentioned above, in order to perform current supply from the personal computer 10 concerned to external peripheral equipment via a USB interface, he branches to the USB driver 110 and is also trying to supply the power supply PWu for USB from the above-mentioned power supply section 114.

[0037]Then, the function as contents managing application started in the personal computer 10 by the above-mentioned composition is typically shown in drawing 5. Greatly, the contents managing application 300 comprises the contents managing program 311, the display operation instruction program 312, the sound recording program 313, and the application program 315 for purchase, and creates and prepares the contents database 314. The contents database 314 is saved at the hard disk 107, for example.

[0038]The contents managing program 311 conceals the contents of processing from the outside, and he is trying for it to become difficult to read and comprehend it of the contents of processing by being described as the instruction shuffled actually, for

example or an enciphered instruction.

[0039]In this contents managing program 311, the EMD selection program 131 is a program provided from the EMD server 1 side via the network 2 by the EMD registration processing performed, for example by a user's prescribed operation. And this EMD selection program 131 is stored for example, in RAM104, and it is made to be held. And selection about connecting with any of EMD servers 1 supposed that the EMD selection program 331 has more than one actually, for example is performed, The application program 315 for purchase or the driver 342 for purchase is made to make connection with this selected EMD server 1.

[0040]Check-in / checkout control program 332, It is what manages operation of check-in/check-out of contents data, If permission is given about the contents as which he checked out when check-out was permitted about the specified contents data, and check-in was required, processing will be performed so that check-in may be performed. The judgment about whether this check-in and check-out are permitted, For example, in the rule of the check-in/check-out explained by drawing 3, and the contents database 314, it is carried out with checking the data content corresponding to the contents data which was the target of check-in/check-out. Check-in / checkout control program 332 updates the contents of the contents database 314 corresponding to processing of check-in or check-out. The structure of the contents database 314 is mentioned later.

[0041]The contents data which the application program 315 for purchase received from EMD server 1 via the network 2 may be enciphered by a method different, for example from the data encryption method performed in this contents managing application 300. The cipher system conversion program 333 is changed into the data format enciphered by the cipher system with which this contents managing application 300 suits about the contents data encryption method which was received from EMD server 1 as mentioned above, and was acquired. As a cipher system to the contents data in this case, a DES (Data EncryptionStandard) method or a FEAL (Fast Encipherment Algorithm) method is employable, for example.

[0042]As contents data which was received and was acquired from EMD server 1, Since compression of audio information may be performed by different compression technology (for example, MP3:MPEG Audio Layer-3 etc.) from ATRAC3 method to which the contents managing application 300 is equivalent, In such a case, conversion to the audio information compressed by ATRAC3 method is made to be performed about the audio information as contents data compressed by the compression technology conversion program 334 with methods other than ATRAC3 method. The

compression technology conversion program 334 also has the function as an encoder which carries out compression processing of the audio information to which compression processing is not performed. For example, it is also made to be performed to perform compression processing by ATRAC3 method about the audio information played from the disk by CD-ROM drive 106 and the audio information which was inputted with the voice input/output interface 108 and acquired.

[0043]The audio information by which the enciphered program 335 was played from the disk, for example with CD-ROM drive 106, When creating the audio information which was inputted with the voice input/output interface 108 and acquired as contents data, it enciphers with the cipher system with which the contents managing application 300 suits.

[0044]Here, it is supposed that the regular player 20 also corresponds the cipher system which suits the contents managing application 300 currently described above, and audio information compression technology. That is, in the player 20, about the contents data to which compression processing and encryption were properly given by the contents managing application 300, elongation processing and code composite-ized processing are performed, audio information is restored, and it is supposed that reproducing properly is possible.

[0045]The format of the utilization condition data (Usage Rule) in which the reproduction condition of the contents data which the utilization condition conversion program 336 received from EMD server 1, and was acquired, copy conditions, etc. are shown, "it changes into the format which can be processed with the contents managing application 300. This utilization condition data is used for creating a contents database.

[0046]The hash value control program 337 computes the hash value about the contents database 314 which has first a data structure mentioned later, and performs processing which stores this for example, to ROM105. The alteration of the utilization condition data in a contents database is detected by referring to a hash value in the preceding paragraph story which performs processing of check-in or check-out. When check-in about a certain contents data or processing of check-out is performed next noting that an alteration is not performed, for example, it also performs updating a hash value. A hash value is obtained by calculating with the application of a hash function to data. It is supposed that it is hard to happen the collision of the hash values from which it changes it into it as a hash function maps variable-length long data in a fixed-length short value and which it is known as a function of tropism on the other hand, and are the result of an operation.

[0047]When the player 20 is actually connected with the personal computer 10 by the USB interface, for example, in the preceding paragraph story which delivers and receives contents data, it is checked whether the contents managing application installed in the personal computer 10 is regular -- both, In order to check whether the player 20 is regular, mutual recognition processing is performed between the personal computer 10 and the player 20. The authentication program 338 is considered as the program which performs authenticating processing which the personal computer 10 side should perform in this mutual recognition processing. Mutual recognition processing with the contents managing program 311 and the application program 315 for purchase and processing of the mutual recognition of the contents managing program 311 and the driver 342 for purchase are performed. Furthermore mutual recognition processing with EMD server 1, the application program 315 for purchase, or the driver 342 for purchase is performed, and for example, ROM103 is made to memorize the authentication key used at this time. This authentication key shall not memorize at the authentication program 338, when the contents managing program 311 is installed in the personal computer 1. And when registration processing is normally performed by the display operation instruction program 312, it is supplied from EMD server 1.

[0048]The decoding program 339 performs performing necessary decoding processing about that contents file, and restoring to audio information, when reproducing contents data on this contents managing application 300. For example, if compression processing is already performed for contents data and encryption is given, audio information will be obtained by solving encryption and performing elongation processing. Thus, the obtained audio information is outputted, for example via the voice input/output interface 108.

[0049]As the power control program 340 is mentioned later, it is established in order to perform power control in the USB driver 110.

[0050]The device driver 341 is the driver software corresponding to the device as the player 20, for example, and manages data transmission and reception with the player 20 through the USB driver 110.

[0051]The driver 342 for purchase is the driver software corresponding to a certain specific EMD server, for example, and is installed as what is called plug-in software to contents managing application 300 main part. Thereby, the transfer of data with the contents managing program 311 of the driver 342 for purchase is attained. And this driver 342 for purchase receives contents data from this EMD server 1 while demanding transmission of predetermined contents data of a certain specific EMD

server 1 via the network 2. Accounting is also made to perform when the driver 342 for purchase receives contents data from this EMD server 1.

[0052]The GUI (Graphical User Interface) program 312, It is considered as the program for realizing GUI as the contents managing application 300, for example, a GUI image is displayed to the display 113 according to operation of the mouse as the operation input section 112, a keyboard, etc.

[0053]The sound recording program 313 is a basis in the state where the window for sound recording is shown by GUI program 312, for example, For example, it is chosen now and audio information of CD with which CD-ROM drive 106 is loaded, or audio information acquired via the voice input/output interface 108 is made into a sound source, It is considered as the program which performs processing for saving as contents data at the hard disk 107. For example, if operation of a recording start is performed to the window for sound recording, the sound recording program 313 saves the audio information as a sound source chosen, for example according to the form of contents data at a hard disk now.

[0054]The contents database 314 comprises a set of the necessary management information file corresponding for every contents data which are managed as a file and saved at the hard disk 107, for example. And it shall be saved to the hard disk 107 also as this contents database 314, for example, a file.

[0055]Here, the example of a data structure of the above-mentioned contents data and the contents database 314 is explained with reference to drawing 8 and drawing 9, respectively. Drawing 8 shows the structure of contents data. As contents data, the header area A1 is first arranged so that it may illustrate, and the data area A2 where audio information is stored after this is arranged. Compression processing is performed by ATRAC3 method, and the audio information stored in the data area A2 is enciphered, for example by predetermined methods, such as DES, so that old explanation may also show.

[0056]Each information on file ID, header size, contents key, file size, codec ID, file name, file information, reproduction restriction data, reproduction opening day, reproduction end date, number-of-times [ of refreshable ], and real reproduction frequency is stored in the header area A1 from a head.

[0057]File ID is ID which becomes peculiar for every file, and header size shows the size of the header area A1. A contents key is further enciphered with a common session key, when it is considered as the data for solving encryption about the audio information of the data area A2 where encryption was given and transfer of contents data is actually performed between the personal computer 10 and the player 20.

[0058]A file size shows the size as a file of this contents data itself, for example, and shows the title as a musical piece of this contents data, and an artist name to file information, for example.

[0059]Codec ID is set to ID which shows the speech compression method given to the audio information as contents data.

[0060]Reproduction restriction data, reproduction opening day, reproduction end date, number-of-times [ of refreshable ], and real reproduction frequency is reproduction restriction management information for reproduction restrictions of the contents data concerned to be performed properly. Copy conditions of a contents database, a value of a copy frequency counter, etc. which reproduction restriction data is made the information which shows the reproduction restrictions set up according to old data transfer and reproduction history after following the rule of SDMI, for example, for example, are mentioned later are reflected. At the time of a reproduction opening day and a reproduction end date, when it is the contents data with reproduction restrictions in which restriction was given during the regeneration phase, the time of the opening day in which the reproduction is enabled, and an end date is shown. Similarly, the number of times of refreshable shows the value of the number of times of refreshable about the contents data with reproduction restrictions in which reproduction frequency is restricted. Real reproduction frequency shows the number of times reproduced by the personal computer 10 or the player 20. Here, when the value which real reproduction frequency shows, for example becomes the same as that of the value of the number of times of refreshable, reproduction of this contents data will be forbidden in the personal computer 10 and the player 20.

[0061]Drawing 9 shows the structure of the contents database. Here, it is assumed that it corresponds as contents data when three of the contents 1-3 are saved at the hard disk 107.

[0062]If it corresponds to each contents as shown in this figure, first, the information on file ID, a contents key, a title, and a file size is established, and utilization condition data is provided further. File ID, a contents key, a title, and a file size have the same contents as what is stored in the header area A1 of the contents data shown in above-mentioned drawing 8 shown.

[0063]The same contents as the number of times of refreshable are shown at the time of a reproduction end date at the time of the reproduction opening day stored in the header area A1 of the contents data which showed drawing 8 ""the time of a reproduction condition:opening day and a reproduction condition:end date"", and ""the number of times of reproduction condition:refreshable"" among utilization condition

data. A "reproduction frequency counter" shows the same contents as the real reproduction frequency stored in the header area A1 of the contents data shown in drawing 8. "They are fee collection conditions at the time of reproduction", the fee collection setups about the contents data concerned are shown. "copy conditions: Number-of-times" shows the copy frequency permitted about the contents data concerned, and if it is a case of this embodiment, number-of-times =3 of check-out will be shown. A "copy frequency counter" shows until now the number of times to which the contents data concerned was copied. For example, the above-mentioned "copy conditions: If the value shown by number-of-times" and the value of a "copy frequency counter" become the same, copying more than this and this contents data will be forbidden. That is, it does not answer [ that there is this contents copy-of-data demand and ], for example in the personal computer 10. in addition -- the case where check-in is performed as for the value of this copy frequency counter -- copy frequency -- a draft -- that value is changed as it lessens. "copy conditions: The copy conditions based on the standard of SCMS (Serial Copy Management System) are shown in SCMS." In SCMS, the copy of only one generation is permitted about performing digital copies, such as audio information, for example from the media of a certain copy origin to the media of a copy destination. The hash value control program 337 (refer to drawing 5) which a hash value is a data row which comprises a predetermined number of bytes, and was mentioned above computes based on the contents of the contents database, and is held, It is referred to when performing the judgment about whether the alteration about the contents of a contents database was performed.

[0064]Then, explanation is returned to drawing 4 and the internal configuration of the player 20 is explained. USB connector 32 shown also in drawing 1 is formed in the player 20, and this USB connector 32 is connected with the internal USB driver 215. In the case of this embodiment, from above-mentioned USB connector 32, the contents data transmitted from the personal computer 10 is inputted into the USB driver 215, and is received here.

[0065]As for the flash memory 206, the beginning of data and read-out are performed by the flash plate memory driver 205. And the contents data received with the USB driver 215 is written in and memorized to the flash memory 206 in this case.

[0066]Here, the contents data memorized by the flash memory 206 is managed by what is called FAT (File Allocation Table). That is, the recording position of the contents data on the flash memory 206 is managed by FAT. Although the data as this FAT may be memorized by the flash memory 206, for example with contents data, it

may be made to memorize it to external ROM210 constituted by EEPROM etc., for example. For example, if FAT is written in external ROM210, the number of times of rewriting to the flash memory 206 supposed that the number of times of rewriting has a limit can be lessened on the structure. It can use for memorizing various setup information etc. to external ROM210, for example.

[0067]When reproducing the contents data memorized by the flash memory 206 as audio information, the specified contents data is first read from the flash memory 205, and it transmits to DSP207 via an internal bus. In DSP207, the audio information stored in the data area A2 from contents data is extracted. And about this audio information, decipherment processing of encryption and data decompression processing are performed, and the digital audio data of a predetermined format are obtained. Signal processing in this DSP207 can also perform adjustment of the tone quality according to the prescribed operation performed, for example to the final controlling element 212, volume, etc. In DSP207 performing signal processing, if there is necessity, for example, the buffer memory 211 will be used as workspace. And the digital audio data produced by doing in this way are outputted to D/A converter 208. In D/A converter 208, the inputted digital audio data are changed into an analog audio signal, and it outputs to the amplifier 209. With the amplifier 209, it amplifies about the inputted analog audio signal, and outputs to the headset jack 22 which is a voice signal output terminal. And if the headphone 40 are connected to the headset jack 22, the sound as a musical piece will be outputted from IYADORAIBA 42 of these headphone 40, for example.

[0068]When [ in which he checks in at the contents data memorized by the flash memory 206 ] getting it blocked, making it move and making and transmitting to the personal computer 10, With the flash plate memory driver 205, the contents data at which he should check in is read from the flash memory 205, and it transmits to the USB driver 215. In the USB driver 215, the transmission output of the contents data is carried out to the USB driver 110 by the side of the personal computer 10 connected via USB connector 32 → USB cable 50.

[0069]As stated also in advance, when the player 20 is connected with the personal computer 10 by the USB interface, perform mutual recognition between the personal computer 10 and the player 20, but. For this reason, the authenticating processing block 204 is formed in the player 20 side. The authenticating processing block 204 performs processing which the player 20 side should perform as mutual recognition processing, for example according to control of CPU201.

[0070]The final controlling element 212 shall comprise the various handlers provided

in the main part 21 of the player 20 shown, for example in drawing 1, and outputs the operation information signal according to the operation performed to the handler. CPU201 performs control management to a various function circuit part based on this operation information signal. Thereby, the necessary operation according to operation is obtained. For example, if operation about reproduction was performed, control to DSP207, reading control to the flash memory 205, etc. will be performed so that necessary reproduction related operation may be performed according to this operation. The display driver 213 performs the drive over the display device as the indicator 30 according to the indicative data outputted from CPU201. Thereby, various kinds of displays are performed in the indicator 30.

[0071]CPU216 begins the various regeneration to the contents data according to the above-mentioned final controlling element, display control, and the communications control through a USB interface, and performs various control management for realizing necessary operation. The data of the program which CPU201 should execute, the initialization information which CPU202 should refer to, etc. are stored in ROM202. The program which CPU201 should execute is started and held and the data which CPU201 used for various processing or an operation is held RAM203.

[0072]The player 20 of this embodiment changes into the voltage of a predetermined level the DC power supply obtained with the battery 217 by the power supply circuit 216, and is made to be used as power supply PW-B of an internal circuit. As mentioned above, from the personal computer 10, it is supposed that it is possible to supply DC power supply voltage outside via USB cable 50. For this reason, when being connected with the personal computer 10 via USB cable 50 as the player 20, the power supply voltage supplied via this USB cable 50 is supplied by the internal circuit. For this reason, power supply PW-U of a predetermined level is obtained from the power supply voltage supplied via USB cable 50 as the USB driver 215 of this embodiment, and it is constituted so that this may be supplied to an internal circuit. Although stopped, suppose the current supply from the power supply circuit 216 which makes the battery 217 a power source at this time that the next explanation is described about the composition of this power-source change.

[0073]As it mentions later, according to the mutual recognition result performed between the personal computer 10 and the player 20, supply of the power supply through a USB interface (USB power supply) is controlled by the system of this embodiment. That is, when it is not attested noting that the player 20 is not apparatus corresponding to a regular system as a mutual recognition result of the personal computer 10 and the player 20. For example, one is made to suspend supply of the

USB power supply from the personal computer 10 to the player 20 as a penalty measure.

[0074]Then, suppose that the example of composition of a power supply circuit system of the personal computer 10 and the player 20 shown in above-mentioned drawing 2 is shown in drawing 6 and drawing 7. Drawing 6 shows the composition of a supply circuit system of a USB power supply as a power supply circuit system in the personal computer 10. To the USB driver 110, the power supply PWu for USB is supplied from the power supply section 114 to the USB driver 110. Here, in the USB driver 110, it shall be provided in the switch 110a in a power supply path, and the above-mentioned power supply PWu for USB is connected to USB connector 111 via the line Vbus from this switch 110a. Here, as for the switch 110a, switch elements, such as FET, are used, for example and an on/off state is controlled by control of CPU102.

[0075]The composition of a power supply circuit system provided in the player 20 side is shown in drawing 7. In the player 20, it is supposed that it is possible to operate considering any of the battery 217 and a USB power supply they are as a power source. First, the battery 217 will be made into a power source in the state where it is not connected with external instruments, such as the personal computer 10, via USB connector 32. In this case, the electric power as DC power supply voltage supplied from the battery 216 is supplied to the power supply circuit 215, It is changed into the direct current voltage stabilized with the predetermined level with DC to DC converter 215a in this power supply circuit 215, and is supplied to necessary circuit elements including for example, CPU201 grade as power supply PW-B. At this time, there is no current supply from the USB power supply side through the USB connector 32 → regulator 216a.

[0076]And suppose that connection with external power feeder machines, such as the personal computer 10, was made via USB connector 32 of the player 20 from the state above-mentioned, for example. Although the data signal by signal-line D+ and D- and the USB power supply by power source line Vbus will be inputted via USB connector 32 at this time, only power source line Vbus which supplies a USB power supply is shown on account of explanation here.

[0077]The USB power supply inputted via USB connector 32 is supplied to the regulator 216a it is supposed that is provided to the inside of the USB detecting-signal generation part 220 and the USB driver 216. In the USB detecting-signal generation part 220, the partial pressure of the voltage of the inputted USB power supply is carried out, the detecting signal which can show that

USB connection was made is generated, and it outputs to DC to DC converter 215a in the power supply circuit 215. If this detecting signal is inputted, it is made for that operation to be stopped by DC to DC converter 215a. That is, when USB connection is made, the current supply which makes the battery 216 a power source by controlling to stop operation of DC to DC converter 215a is made not to be performed. And power supply PW-U produced by transforming into predetermined level voltage the USB power supply inputted by the regulator 216a instead of this is made to be supplied to an internal circuit.

[0078]Here, it is switched to the state where make it DC to DC converter 215a have operation started, and battery-operated is carried out again, instead of supply of power supply PW-U through the regulator 216a being suspended if it changed into the state where USB connection was removed from the state above-mentioned, for example.

[0079]5. As a data transfer processing 5-1. check-out processing book embodiment, even if it describes above, have the feature in the USB power control according to a mutual recognition processing result so that it may be, but. It performs in order to check whether its each is regular when mutual recognition processing performs data transfer between the personal computer 10 and the player 20. Then, next, the processing operation at the time of data transfer including this mutual recognition processing is explained. The data copy from the personal computer 10 called "check-out" with having mentioned above as data transfer of this embodiment to the player 20, Since data movement (move) from the player 20 called "check-in" to the personal computer 10 is performed, this check-out processing and check-in processing are explained one by one.

[0080]The processing operation for check-out is shown in drawing 10 and drawing 11. The flow chart shown in this figure shall show the processing at the time of seeing from the personal computer 10 side, and CPU102 shall be performed according to the program of contents managing application.

[0081]When checking out, the hash value corresponding to the contents of the present whole contents database is first calculated in Step S101 of drawing 10. And in the following step S102, it compares about the hash value which it is computed in the hash value obtained at the above-mentioned step S101, and last time, for example, was made to hold to ROM103, and it is distinguished whether the value is in agreement. Here, when a negative result is obtained noting that both hash value is not in agreement, it progresses to Step S103, the message which shows not checking out since the contents database may have been altered unjustly is displayed, and this

routine is terminated. On the other hand, when an affirmation result is obtained noting that both hash value is in agreement in Step S103, it progresses to Step S104.

[0082]In Step S104, the information on each contents registered there is read from the contents database saved at the hard disk 107, for example. And control management for displaying the GUI image for choosing contents data (that is, it is a musical piece) to the display 113 based on this read information is performed. The user can choose the contents which should be checked out by operating it to the GUI image for this contents selection, for example using the operation input section 12.

[0083]Supposing a decision of the contents data which should be checked out is made by the user's operation which is said to have been carried out, for example in the above-mentioned step S105 here, [ in a contents database ] in continuing Step S105, the utilization condition data corresponding to this selected contents data is checked. That is, fee collection conditions etc. are investigated at the time of the various reproduction conditions about selected contents data, copy conditions, and reproduction. And in the following step S106, it is distinguished whether based on the checked result of each above-mentioned utilization condition data, he can check out about selected contents. Here, when it is distinguished noting that check-out should be forbidden, this routine is ended, but when you can check out, it progresses to Step S107.

[0084]In continuing Step S107, mutual recognition processing between the players 20 of the personal computer 10 is performed.

[0085]Although the details of this mutual recognition processing are mentioned later, If it explains briefly here, the master key KM shall be beforehand memorized by external ROM210 of the player 20, and ID which specifies the apparatus as the individual key KI and the personal computer 10 concerned shall be beforehand memorized by ROM103 of the personal computer 10, for example. In the player 20 side, ID transmitted from the personal computer 10 side receives, a hash function is applied to the master key KM held by the ID and player 20 side, and the same key as the individual key it is supposed that is held to ROM103 by the side of the personal computer 10 is generated. The personal computer 10 and an individual key common to both players 20 will be shared between doing in this way. A still more nearly temporary key for communication is generable using this individual key.

[0086]Or while, making ROM103 of the personal computer 10 memorize ID and master key KM1 beforehand for example, it is made to make external ROM210 of the player 20 memorize ID of the player 20, and master key KM2 as other authenticating processings. And by transmitting each ID and master key of each other to another

side, another side applies a hash function to ID and the master key which have been transmitted from one side, and generates the individual key of another side. And it may be made to generate a temporary key for communication further from the individual key.

[0087]And in the above-mentioned step S107, when attestation is obtained mutually, after the player 20 of the personal computer 10 shares the above-mentioned temporary key for communication (momentary key Ks) eventually, it shifts to Step S108. Processing when mutual recognition is not obtained is mentioned later.

[0088]In Step S108, the information which the file as contents data of file ID etc. can specify is read from a contents database. And in the following step S109, processing which changes into the thing corresponding to the player 20 a compression encoding system of audio information and a cipher system, a format, etc. which are included in the contents data acquired by the above-mentioned step S108 is performed if necessary. However, this processing will be skipped if considered as the compression encoding system corresponding to the player 20 and the cipher system, and the format in the stage saved at the hard disk 107. After processing of this step S109 is completed, it shifts to processing of Step S110 of drawing 11.

[0089]In Step S110, the contents data which was read and was acquired from the hard disk 107 is enciphered with the key for communication (momentary key) shared by mutual recognition processing of previous Step S107. And it transmits via a USB interface to the player 20. The contents data transmitted as mentioned above is received, and it writes in the flash memory 206 and is made to memorize in the player 20 side.

[0090]In the following step S111, each reproduction condition (at the time [ At the time of an opening day ] of an end date number of times of refreshable) of the contents database corresponding to selected contents data is changed into the form that the player 20 is manageable, if necessary. In Step S112 which furthermore continues, the SCMS information in the copy condition of the contents database corresponding to selected contents data is changed into the form which the player 20 manages. And in the following step S113, the above-mentioned step S111, and the reproduction condition and SCMS information which were changed by processing of S112 are transmitted to the player 20. In the player 20 side, the reproduction condition and SCMS information which were received are saved to flash memory 206 or external ROM210.

[0091]In the following step S114, fee collection conditions, copy conditions, etc. are transmitted to the player 20 with the form which CPU102 is treating at the time of the

various reproduction conditions and reproduction which are utilization condition data registered into the contents database of selected contents. In the player 20 side, the transmitted utilization condition data will be saved to flash memory 206 or external ROM210.

[0092]In [ read the encryption key which has enciphered selected contents data in the following step S115, i.e., a contents key from a contents database, and ] Step S116, The contents key is decoded with the key for preservation memorized by ROM103, and it enciphers with the key for communication. And this contents key enciphered with the key for communication is transmitted to the player 20. In the player 20 side, the encryption key transmitted from the personal computer 10 is decoded by processing of the authenticating processing block 204 which CPU201 controls using the key for communication shared between mutual recognition processing, and it enciphers using its own key for preservation. And it relates with the already saved data and saves to flash memory 206 or external ROM210. Thus, header information, including contents data, utilization condition data, etc., is transmitted from the personal computer 10 to the player 20 one by one, and data transfer as check-out is performed by receiving and memorizing this in the player 20 side.

[0093]And in the following step S117, one copy frequency counter of the contents database corresponding to the contents data transmitted to the personal computer 10 side is \*\*\*\*\*ed. By processing of the above-mentioned step S117, the contents of the contents database differ from the former. Then, in the following step S118, the operation about the hash value of the whole contents database is performed, and this newly obtained hash value is held to ROM103. That is, the update process of a hash value is performed.

[0094]5-2. Explain the processing operation for check-in processing, then check-in with reference to the flow chart of drawing 12. In this figure, one flow shows the processing by the side of the personal computer 10, and the processing by the side of the player 20. According to the program of contents managing application, CPU102 performs processing by the side of the personal computer 10, and CPU201 performs processing by the side of the player 20.

[0095]In the processing shown in this figure, read-out of the management information about the contents data memorized by the flash memory 206 of the player 20 from the personal computer 10 to the player 20 is first required in Step S201. With management information here, the information, including the contents, FAT, etc., stored in the header of contents data, for example is comprised, and it is considered as the information used for the record reproduction management about the contents data

memorized by the flash memory 206. And according to this demand where this management information is saved, for example in external ROM210 or the flash memory 206, CPU201 of the player 20 performs control management for reading the memorized management information and transmitting to the personal computer 10. In the personal computer 10 side, the GUI image for choosing the contents data as a musical piece memorized by the player 20 side based on the management information which received is displayed on the display 113. The user can choose the contents data which should be made to check in by operating it to this GUI image.

[0096]And supposing a decision of the contents data which should be made to check in in the above-mentioned step S201 is made, mutual recognition processing by the side of the personal computer 10 and the player 20 will be performed by processing as continuing Step S202. This processing is made to be the same as that of processing of Step S107 previously shown in drawing 10.

[0097]From the inside of the continuing contents data which is memorized by the flash memory 206 in Step S203, read-out about contents data by which selected designation was carried out for check-in is performed, and it transmits to the personal computer 10. In the personal computer 10 side, by processing of continuing Step S204, a file name is given to the contents data transmitted from the player 20, and it saves as a file at the hard disk 107.

[0098]Next, in the player 20 side, read-out about the encryption key which has enciphered the contents data at which he should check in this time by processing of Step S205 is performed. For example according to processing of Step S116 previously shown in drawing 10, the player 20 side saves this encryption key at the flash memory 206. And in the player 20 side, after decoding the encryption key which read using the key for preservation which he has and enciphering with the key for communication further, a transmission output is carried out to the personal computer 10.

[0099]In the personal computer 10, processing of Step S206 receives the encryption key transmitted by the above-mentioned step S205 from the player 20, this received encryption key is decoded with the key for communication, and it enciphers with the key for preservation which he has further. And in the following step S207 the personal computer 10, The file name etc. of the contents data saved at previous Step S204. For example, the encryption key etc. which were enciphered at file information, such as a title and an artist name, and the above-mentioned step S206 which are said for you to have inputted by GUI operation are registered into the contents database held now. And in continuing Step S208, updating about the hash value of the whole contents database is performed. That is, the hash value corresponding to the

contents database with which the contents were rewritten by processing of the above-mentioned step S207 is computed, for example, ROM103 is made to memorize. [0100]In the following step S209, it reports that the encryption key was saved to the player 20, and the personal computer 10 side requires deletion of the contents data made to check in this time. And in the player 20, according to the communication from the personal computer 10 as the above-mentioned step S209 by processing as Step S210. The contents data at which he checked in this time is deleted from the inside of the contents data memorized by the flash memory 206. It means that movement of contents data in the personal computer 10 from the player 20 was performed by this. That is, the operation as check-in will be obtained.

[0101]6. Explain mutual recognition processing and source control processing, then the mutual recognition processing previously shown as Step S107 of drawing 10, and Step S202 of drawing 12 with reference to the flow chart of drawing 13 and drawing 14. As this embodiment, when attestation is not obtained as a mutual recognition processing result, supply control of a USB power supply is performed, but the processing for this power supply control is also included here. Processing of both of the personal computer 10 and player side is shown here, the personal computer 10 performs processing of Steps S301–S311, and the player 20 performs processing of Steps S321–S332 (or S333). According to the authentication program 338, CPU102 performs processing by the side of the personal computer 10 as processing shown in this figure, and processing by the side of the player 20 is performed because CPU201 controls the authenticating processing block 204. USB power supply control in the personal computer 10 according to an authenticating processing result is performed according to the power control program 340.

[0102]In mutual recognition processing, first by processing as Step S301 of drawing 13. Random number Na is generated to the personal computer 10 side, and processing for transmitting ID of the personal computer 10, category number [ of a key ] G, and above-mentioned random number Na to the player 20 is performed in the following step S302.

[0103]On the other hand, the player 20 generates the random number Nb in Step S321, and receives ID of the personal computer 10 transmitted from the personal computer 10, category number [ of a key ] G, and random number Na in the following step S322. And in the following step S323, the key number j of the master key KMa is acquired from category number [ of a key ] G.

[0104]By processing of Step S324 which continues in the player 20 side. The key Kab is computed by asking for the j-th master key KMa [j], and applying the hash function

based on the master key  $KMa [j]$  to ID of the personal computer 10 in the following step S325. In continuing Step S326, the random number  $R1$  is computed with the application of the hash function based on the key  $Kab$  to ID of random number  $Na$ , the random number  $Nb$ , and the personal computer 10. The random number  $Sb$  is generated depending on the following step S327.

[0105]And in the following step S328, control management for transmitting random number  $Na$ , the random number  $Nb$ , the key number  $j$ , and the random number  $Sb$  which were obtained by old processing to the personal computer 10 is performed. After processing of Step S328 follows the player 20 to processing of Step S329 of drawing 14.

[0106]In the personal computer 10, the processing as Step S303 receives random number  $Na$ , the random number  $Nb$ , the key number  $j$ , and the random number  $Sb$  which have been transmitted by processing of the above-mentioned step S328 from the player 20. Then, the personal computer 10 shifts to Step S304 of drawing 14.

[0107]In the following step S304, processing for obtaining the key  $Kab$  contained in the individual key  $KIa$  based on the key number  $j$  received and acquired is performed in the personal computer 10. In the following step S305, the random number  $R2$  is computed by applying the hash function based on the key  $Kab$  to ID of random number  $Na$  [ which is held now ], random number  $Nb$ , and personal computer 10 self.

[0108]And in the following step S306, it is distinguished in the personal computer 10 whether the received random number  $R1$  and the random number  $R2$  generated at the above-mentioned step S305 are equal. Here, when an affirmation result is obtained, it will be supposed that it is the player which is the other party of mutual recognition the regular player 20. In this case, it progresses to the processing after Step S307. On the other hand, when a negative result is obtained, the player which is the other party of mutual recognition will be attested as the regular player 20. In this case, it progresses to Step S311. Processing of Step S311 is mentioned later.

[0109]The personal computer 10 generates the random number  $Sa$ , and computes the random number  $R3$  with the application of the hash function based on the key  $Kab$  to the random number  $Nb$  and random number  $Na$  in Step S307 in continuing Step S308. In the following step S309, the transmission output of the above-mentioned random number  $R3$  and the random number  $Sa$  is carried out to the player 20. And in Step S310, it asks for the key  $Ks$  with the application of the hash function based on the key  $Kab$  from the random number  $Sa$  and the random number  $Sb$  temporarily.

[0110]In [ on the other hand by the player 20 side, processing of Step S329 receives the random number  $R3$  and the random number  $Sa$  which were transmitted by

processing of Step S309 from the personal computer 10 side, and ] the following step S330, With the application of the hash function based on the key Kab, the random number R4 is computed to the random number Nb and random number Na.

[0111]And in continuing Step S331, the judgment about whether the received random number R3 and the random number R4 generated at the above-mentioned step S330 are equal is performed. Here, when judged with the random number R3 and the random number R4 not being equal, attestation that the personal computer 10 of the other party is the apparatus which installed regular contents managing application, for example will be performed. And check-in with the inaccurate personal computer 10 connected by ending subsequent processings here, for example now, for example and check-out are made not to be performed. on the other hand, when it judges with the random number R3 and the random number R4 being equal by Step S331, the personal computer 10 is the apparatus which installed regular contents managing application -- it means that it was attested and is made to progress to processing of Step S332. When it does not attest in Step S331, it is also possible to proofread so that it may progress to processing of Step S333, but this is mentioned later.

[0112]It enables it to ask for the key Ks with the application of the hash function based on the key Kab from the random number Sa and the random number Sb in Step S332 temporarily. Thus, when mutual recognition processing is performed and both sides are attested, as mentioned above, the key Ks can be obtained by the personal computer 10 and the player 20 temporarily which is a common key for communication.

[0113]It progresses to Step S311 performed as processing by the side of the personal computer 10 when the player 20 is not attested, and processing for the supply control of the USB power supply by the side of the personal computer 10 is performed.

[0114]As supply control of the USB power supply by Step S311 as this embodiment, it is possible several kinds. Then, some of actual examples of the power supply control considered in the system of this embodiment below will be given.

[0115]CPU102 sets the switch 110a (refer to drawing 6) in the USB driver 110 to OFF as processing of Step S311 one, for example. That is, the operation which supplies a USB power supply to the player side via Vbus is stopped. And subsequent processings are made not to perform, for example. That is, if it is original, the transmission and reception of contents data performed after mutual recognition processing shall not be carried out.

[0116]When processing as such a step S311 is performed, in addition to data communications no longer ceasing to be performed by software, supply of a USB power supply will also be suspended with the player of the other party made not

regular, for example. Thereby, an inaccurate player can be eliminated more firmly than the case where data communications are forbidden, and copyright protection is also only strengthened so much by software-based control, for example.

[0117]After making one suspend like the above the operation which supplies a USB power supply to the player side via Vbus in Step S311, it is made to be returned to Step S407 from Step S311 in drawing 14, as a dashed line shows. Subsequent processings are making it continue, and even if the player of a jam of the other party is inaccurate, if data communication processing is possible, it will perform this.

[0118]In this case, if this player made not regular is the composition in which battery-operated is possible, data communications will be made possible, for example. That is, it becomes possible to make only a certain period of inside with the residue of a battery check out contents data etc. That is, in this case, the above is making the protection to an inaccurate player loose conversely, and convenience to a user is planned suitably.

[0119]The following USB power control is also considered. Although the graphic display of the concrete composition of a power supply circuit system for this is omitted, it is made to drop the power supply voltage of the USB power supply supplied via Vbus of a USB interface, for example as processing of Step S311 even to a predetermined level rather than regulation. For example, in the player side, it is common that a direction when writing in needs much electric power in the time of writing the contents data in which he was checked out in media, such as a flash memory, and the time of reading contents data from media and reproducing. Therefore, if it controls to reduce the voltage level supplied as a USB power supply as mentioned above, in the player side, only reproduction of contents data can be performed and the writing to media will be made able [ carrying out ] to prevent. That is, it becomes possible to obtain the limiting action in the gestalt of forbidding only the recording operation by the side of a player. Thus, according to this embodiment, it is supposed that it is possible to realize copyright protection by various gestalten by the method of USB power supply control.

[0120]It is possible for it to be made to perform USB power control to the player 20 side, for example. A jam so that it may be shown as Step S333 as processing by the side of the player 20 in drawing 14, When it does not attest noting that it is regular in the personal computer 10 in Step S331, it controls not to supply the USB power supply supplied, for example to the player 20 side to an internal circuit. For the purpose, what is necessary is just to stop operation of the regulator 216a by control of CPU201, for example. Or the above-mentioned example is imitated, and although

reproduction is possible, it may be made to reduce the voltage level of power supply PW-U outputted from the regulator 21, by the time record is made improper. When stopping supply to the internal circuit of a USB power supply, in consideration of the situation how much to actually plan copyright protection to, for example, it should just be determined whether it has composition which supplies power supply PW-B which makes the battery 216 a power source to an internal circuit. Anyway, if it is performed above, he will check in using the personal computer which is not regular, it will become possible to give restriction to the user who is trying to check out, and copyright protection will be planned.

[0121]It is not limited to the composition shown as the above-mentioned embodiment as this invention, and you may be changed suitably. For example, as an embodiment, although data transmission and reception as check-in/check-out shall be performed by the personal computer and the portable audio player, as two or more set machine which performs data transmission and reception, it is not limited to these. For example, it replaces with a personal computer and may be considered as the apparatus corresponding to EMD for exclusive use which became a portable audio player and a set, etc. It is not limited to a built-in flash memory as media to which the apparatus which becomes the portable audio player side corresponds, and various disk media besides the memory device which can be inserted and detached, for example on a main part etc. may be adopted. It may not be limited, for example to a portable type, for example, you may be considered as a non-portable audio player. It is not limited to USB as an interface which performs data transmission and reception among these apparatus, and with data, if it is an interface in which current supply is possible, this invention is applicable. It may be considered as the actual condition of the check-out processing shown with each figure, check-in processing, and mutual recognition processing, or you may be changed suitably.

[0122]

[Effect of the Invention]As explained above, this invention, for example a personal computer and a portable audio player, As it copies or moves, transmit and receive the data from which it connects with the data interface in which current supply, such as USB, is possible, and copyrights, such as audio information, should be protected, and. In the information transmission and reception system to which the power supply was supplied from the personal computer to the portable audio player, mutual recognition is made to be performed between these two apparatus. And according to this authentication result, the power supply supplied via a data interface is made to be controlled. That is, it is controlling current supply as this invention according to an

authentication result, and the transmission and reception operations of data, etc. are restricted. Thereby, as compared with the case where data-transmission-and-reception control and function restriction control are carried out only to software-based processing, for example according to an authentication result, the limiting action of data transmission and reception with the pliability of a certain grade can be obtained. That is, it is supposed that it is possible to realize easily copyright protection which is various in level with the hardware technique of power supply control. Since data transmission and reception will be restricted in hardware as this invention, it becomes possible to, also make a software-based processing burden ease for example.

2.\*\*\*\* shows the word which can not be translated.

3.In the drawings, any words are not translated.

---

## DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]

[Drawing 1]It is an explanatory view showing the example of composition of the data transmission and reception system as an embodiment of the invention.

[Drawing 2]It is an explanatory view showing the usage pattern of the data transmission and reception system of this embodiment.

[Drawing 3]It is an explanatory view explaining the rule of the check-in/check-out in the data transmission and reception system of this embodiment.

[Drawing 4] They are a personal computer which is a data transmission and reception system of this embodiment, and a block diagram showing the circuitry of a player.

[Drawing 5] It is a block diagram showing the function of the contents managing application installed in a personal computer.

[Drawing 6] It is a block diagram showing the composition of a power supply circuit system of a personal computer.

[Drawing 7] It is a block diagram showing the composition of a power supply circuit system of a player.

[Drawing 8] It is an explanatory view showing the structure of contents data.

[Drawing 9] It is an explanatory view showing the structure of a contents database.

[Drawing 10] It is a flow chart which shows the processing operation for check-out.

[Drawing 11] It is a flow chart which shows the processing operation for check-out.

[Drawing 12] It is a flow chart which shows the processing operation for check-in.

[Drawing 13] It is a flow chart which shows mutual recognition processing.

[Drawing 14] It is a flow chart which shows mutual recognition processing.

[Description of Notations]

1 An EMD server and 2 A network and 10 Personal computer, 20 portable-audio player, 32 USB connectors, 102 CPU, 107 A hard disk, a 110USB driver, 111 USB connectors, 114 A power supply section, 201 CPU, and 204 [ A battery and 314 / A contents database, 338 authentication programs, and 340 / Power control program ] An authenticating processing block and 206 A flash memory, 207 DSP, and 216 A power supply circuit and 217

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-243707

(P2001-243707A)

(43) 公開日 平成13年9月7日(2001.9.7)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード*(参考)
G 1 1 B 20/10		G 1 1 B 20/10	H 5 B 0 1 1
G 0 6 F 1/26		G 0 6 F 12/14	3 2 0 A 5 B 0 1 7
12/14	3 2 0	1/00	3 3 0 F 5 D 0 4 4

審査請求 未請求 請求項の数 3 O L (全 23 頁)

(21) 出願番号 特願2000-54129(P2000-54129)

(22) 出願日 平成12年2月29日(2000.2.29)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 細萱 則文

東京都品川区北品川6丁目7番35号 ソニ

ー株式会社内

(74) 代理人 100086841

弁理士 脇 篤夫

Fターム(参考) 5B011 DA01 DA06 DB21 EA02 EA10

EB03 HH02 MA06 MB13 MB18

5B017 AA03 AA06 CA15 CA16

5D044 AB05 BC01 BC03 CC04 HL11

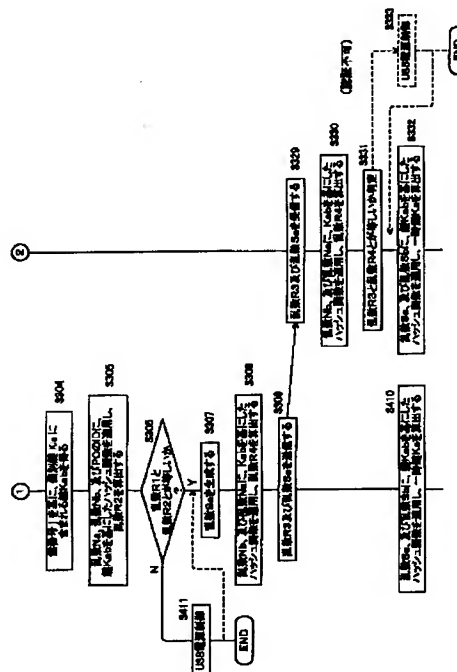
HL20

(54) 【発明の名称】 情報送受信システム、及び電子機器

(57) 【要約】

【課題】 システムにおける著作権保護のための動作制限について多様性を得る。

【解決手段】 パーソナルコンピュータと携帯型オーディオプレーヤとをUSBケーブルにより接続し、オーディオデータなどの著作権が保護されるべきデータを、コピー、もしくは移動するようにして送受信すると共に、パーソナルコンピュータから携帯型オーディオプレーヤに対して電源を供給するようにされた情報送受信システムにおいて、この2つの機器間で相互認証を行うようにされる。そしてこの認証結果に応じて、USBケーブルを介して供給される電源の制御を行うようにされる。



## 【特許請求の範囲】

【請求項 1】 複数のコンテンツ情報を記憶可能とされる第 1 の記憶手段と、

接続された外部電子機器との情報の送受信と、接続された外部電子機器への電源供給とが可能な第 1 の接続手段と、

を備える第 1 の電子機器と、

複数のコンテンツ情報を記憶可能とされる第 2 の記憶手段と、

上記第 1 の電子機器と接続されることで、上記第 1 の電子機器との間での上記コンテンツ情報を含む情報の送受信、及び上記第 1 の電子機器から供給される電源を入力して内部回路に供給可能な第 2 の接続手段と、

を備える第 2 の電子機器と、

を有して成ると共に、

上記第 1 の接続手段と上記第 2 の接続手段によって接続される第 1 の電子機器と第 2 の電子機器とについて相互認証処理を実行する相互認証処理手段と、

上記相互認証処理の認証結果に応じて、上記第 1 の電子機器から上記第 2 の電子機器の内部回路への電源供給を制御する電源制御手段と、

を備えることを特徴とする情報送受信システム。

【請求項 2】 複数のコンテンツ情報を記憶可能とされる記憶手段と、

接続された外部電子機器との情報の送受信と、接続された外部電子機器への電源供給とが可能な接続手段と、

上記接続手段によって接続される外部電子機器とについて相互認証処理を実行する相互認証処理手段と、

上記相互認証処理の認証結果に応じて、外部電子機器への電源供給を制御する電源制御手段と、

を備えることを特徴とする電子機器。

【請求項 3】 複数のコンテンツ情報を記憶可能とされる記憶手段と、

接続された外部電子機器との情報の送受信と、接続された外部電子機器から供給される電源を入力して内部回路に供給可能な接続手段と、

上記接続手段によって接続される外部電子機器とについて相互認証処理を実行する相互認証処理手段と、

上記相互認証処理の認証結果に応じて、上記外部電子機器から供給される電源の内部回路への供給を制御する電源制御手段と、

を備えることを特徴とする電子機器。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、例えばオーディオデータなどのコンテンツ情報の送受信を行う電子機器より構成される情報送受信システム、及びこの情報送受信システムを構成する電子機器に関するものである。

## 【0002】

【従来の技術】 近年におけるパーソナルコンピュータの

利用形態として、例えば CD (Compact Disc) もしくは他の記録媒体から再生したオーディオデータをハードディスクなどの記憶媒体にファイルとして保存したり、あるいは、インターネットのサイトなどからオーディオデータをダウンロードして、これをハードディスクにファイルとして保存することが行われている。

【0003】 また、このようにして、パーソナルコンピュータのハードディスクに保存したオーディオデータのファイルを利用することのできるオーディオプレーヤとして、例えば内部にフラッシュメモリなどの記録媒体を備えることで、大幅な小型化が図られた携帯型オーディオプレーヤも普及してきている。

【0004】 上記した携帯型オーディオプレーヤを利用するのにあたっては、例えばユーザは、パーソナルコンピュータと携帯型オーディオプレーヤとを所定のデータバスを介して接続し、パーソナルコンピュータのハードディスクに保存されているオーディオファイルを転送して、携帯型オーディオプレーヤのフラッシュメモリに書き込んで記録する。そして携帯型オーディオプレーヤ側でフラッシュメモリに記録されたオーディオデータを再生してこれを例えばヘッドフォンなどを接続して聴くようにされる。

## 【0005】

【発明が解決しようとする課題】 ところで、例えば上記したようなパーソナルコンピュータと携帯型オーディオプレーヤとから成るシステムでは、記録媒体間でデータのコピー（複製）や移動などのデータ転送が行われることになる。従って、著作権保護の観点からみた場合には、或る程度、データの転送が制限されるようにする必要がある。すなわち無制限にデータ転送を許可してしまうと、著作権を侵害する可能性がでてくるものである。その一方で、一般のユーザが上記のような使用形態を楽しめるようにするため、完全にデータ転送を禁止してしまうことは適切ではない。従って、著作権保護を図りながらも、ユーザの私的利用範囲内で認められている程度のデータの複製は可能とされるような、或る程度の柔軟性を有したデータ転送管理が行われるようにされることが求められている。

## 【0006】

【課題を解決するための手段】 そこで本発明は上記した課題を考慮して次のように構成する。先ず、情報送受信システムとしては、複数のコンテンツ情報を記憶可能とされる第 1 の記憶手段と、接続された外部電子機器との情報の送受信と、接続された外部電子機器への電源供給とが可能な第 1 の接続手段とを備える第 1 の電子機器と、複数のコンテンツ情報を記憶可能とされる第 2 の記憶手段と、第 1 の電子機器と接続されることで第 1 の電子機器との間でのコンテンツ情報を含む情報の送受信及び第 1 の電子機器から供給される電源を入力して内部回路に供給可能な第 2 の接続手段とを備える第 2 の電子機

器とから成るものとする。そして第1の接続手段と第2の接続手段によって接続される第1の電子機器と第2の電子機器とについて相互認証処理を実行する相互認証処理手段と、相互認証処理の認証結果に応じて第1の電子機器から第2の電子機器の内部回路への電源供給を制御する電源制御手段とを備えることとした。

【0007】また、複数のコンテンツ情報を記憶可能とされる記憶手段と、接続された外部電子機器との情報の送受信と、接続された外部電子機器への電源供給とが可能な接続手段と、この接続手段によって接続される外部電子機器とについて相互認証処理を実行する相互認証処理手段と、相互認証処理の認証結果に応じて、外部電子機器への電源供給を制御する電源制御手段とを備えて電子機器を構成することとした。

【0008】また、複数のコンテンツ情報を記憶可能とされる記憶手段と、接続された外部電子機器との情報の送受信と、接続された外部電子機器から供給される電源を入力して内部回路に供給可能な接続手段と、この接続手段によって接続される外部電子機器とについて相互認証処理を実行する相互認証処理手段と、相互認証処理の認証結果に応じて外部電子機器から供給される電源の内部回路への供給を制御する電源制御手段とを備えて電子機器を構成することとした。

【0009】上記各構成によれば、2つの電子機器を互いの接続手段により接続することで、コンテンツ情報の送受信と、一方の電子機器から他方の電子機器への電源供給が行われるという情報送受信システムが構成され、情報の送受信にあたっては、例えば互いの電子機器がコンテンツ情報の送受信規格に準拠したものであるか否かを判定する相互認証が行われる。そして、認証結果に応じて、上記した一方の電子機器から他方の電子機器への電源供給を制御するように構成されるのであるが、これによって、例えば認証されない電子機器の動作を、電源制御によって制限するということが可能となるものである。

#### 【0010】

【発明の実施の形態】以下、本発明の実施の携帯について説明する。なお、以降の説明は次の順序で行う。

#### 1. 情報送受信システム

##### 1-1. 全体構成

##### 1-2. システムの利用形態

##### 1-3. 内部構成

#### 5. データ転送処理

##### 5-1. チェックアウト処理

##### 5-2. チェックイン処理

#### 6. 相互認証処理及び電源制御処理

#### 【0011】1. 情報送受信システム

##### 1-1. 全体構成

図1は、本発明の実施の形態としての情報送受信システムの全体構成を概略的に示している。本実施の形態の情

報送受信システムとしては、例えばユーザが所有する、パーソナルコンピュータ10と、ポータブルオーディオプレーヤ（以降、単にプレーヤともいう）20から成る。

【0012】この場合、パーソナルコンピュータ10は、プレーヤ20に転送すべき楽曲としてのコンテンツデータを取得して、例えばハードディスクなどのストレージデバイスに対してファイルとして保存するための機器として利用される。そして、コンテンツデータの取得にあたっては、大きくは次の2つの方法が挙げられる。

【0013】1つには、ここでは図示していないが、パーソナルコンピュータ10に備えられる音声入出力インターフェイスを介して取り込んだオーディオデータや、CD-ROMドライブなどによりCDフォーマットのディスクメディアから再生したオーディオデータをコンテンツデータとして取得するものである。

【0014】また、1つは、ネットワークを介して配信される楽曲としてのコンテンツデータをダウンロードして取得する方法である。パーソナルコンピュータ10は、例えばインターネットなどのネットワークを介してEMD(Electrical Music Distribution)サーバ1と通信可能とされている。EMDサーバ1においては、配信のための多数のコンテンツデータが格納されている。ここでのコンテンツデータは、楽曲としてのオーディオデータとされる。そして、例えばパーソナルコンピュータ10のユーザは、パーソナルコンピュータ10に対する操作によって、購入すべき楽曲としてのコンテンツデータを選択する。そして、購入するコンテンツデータを決定すると、パーソナルコンピュータ10では、このコンテンツデータの配信をEMDサーバ1に対して要求する。EMDサーバ1では、この要求に応じた楽曲のコンテンツデータをパーソナルコンピュータ10に対して送信出力する。パーソナルコンピュータ10では、コンテンツデータを受信して保存する。

【0015】なお、本実施の形態のパーソナルコンピュータ10としては、上記のようにしてコンテンツデータを取得してファイルを保存する機能のほか、後述するようにして、パーソナルコンピュータ10とプレーヤ間でコンテンツデータの授受を行う際の著作権保護を図るための著作権保護機能を有する。著作権保護機能としては、例えば暗号化機能やコンテンツデータ送受信時の認証処理機能などが与えられる。そして、このような機能は、例えばプレーヤ20の製造メーカが提供するコンテンツデータを管理するためのアプリケーションソフトウェア（以下、「コンテンツ管理アプリケーション」という）をパーソナルコンピュータ10にインストールすることで得られる。また、上記コンテンツ管理アプリケーション、及び本実施の形態のプレーヤ20が対応するコンテンツデータは、A T R A C (Adaptive Transform Acoustic Coding)方式を改良したA T R A C 3といわれる

方式により圧縮処理されたオーディオデータとされる。なお、実施の形態としてはこの圧縮方式に限定される必要はない。また、パーソナルコンピュータ10には、周辺機器とのデータインターフェイスの1つとして、USB(Universal Serial Bus)が設けられ、次に説明するプレーヤ20とはUSBによって通信可能に接続される。

【0016】プレーヤ20は携帯型のサイズ形状を有して、ユーザが持ち運びながらコンテンツデータを再生して聴くことのできるオーディオプレーヤであり、楽曲としてのコンテンツデータを記録再生するメディアとしてフラッシュメモリを内蔵している。

【0017】プレーヤ20の本体21の上側平面部には、ヘッドフォンジャック22が設けられており、ここに対して、ヘッドフォン40のヘッドフォンプラグ41を差し込んでイヤドライバ42を耳に装着することで、ユーザは再生されたコンテンツデータを音声として聴くことができる。また、同じ本体21の上側平面部には、円柱形状の操作ボタン23が設けられる。この操作ボタン23は、所定の押圧操作、回転操作を行うことで、コンテンツデータの再生／一時停止、頭出し、早送り／早戻し等の操作を行うことが可能とされている。また、本体21の側面部には、ボリュームキー24、低音／音量制限キー25、ホールドキー26が設けられている。ボリュームキー24はヘッドフォン40により聴くことのできる音声の音量レベルを調節するもので、低音／音量制限キー25は、所定操作を行うことで、低音域のレベル調整、及び最大音量を或る所定レベルに制限する機能のオン／オフ設定を行う。ホールドキー26は、プレーヤ20に設けられる操作子に対する操作を無効としたい場合に使用する。音量制限キー25は、例えば電車内などの公共の場で、周囲に音声は漏れて迷惑をかけないようにしたい場合などに使用し、また、ホールドキーは、不用意に本体の操作キーに対する操作が行われてしまうのを防ぎたい場合に使用する。

【0018】また、本体21側面の正面とされる面においては、表示部30、プレイモードキー27、ディスプレイキー28が設けられる。表示部30には、プレーヤ20の動作状況に応じた所定の表示が行われる。例えば、再生中には、現在の動作状態、曲番、経過時間等が表示される。また、ディスプレイキー28を操作することで、この表示部30における表示内容を変更することができ、例えば、ディスプレイキー28を操作した場合には、曲番、経過時間を表示している状態から、曲名、アーティスト名などを表示する状態に切り換えたり、再生信号レベルをスペクトラムアナライザ的に示す表示とコンテンツデータのビットレートを表示する状態に切り換えたりすることが可能とされる。プレイモードキー27は、例えば1曲リピート再生、全曲リピート再生、シャッフル再生などの特殊再生モードを設定するために設けられ、このキー操作によって設定された特殊再

生モードも、例えば表示部30におけるセグメント表示による所定の表示形態によって示される。

【0019】また、ボリュームキー24等が設けられている本体21の側面部の下側には、USBコネクタ32が設けられる。このUSBコネクタ32は、USBケーブル50によりパーソナルコンピュータ10と通信可能に接続するために設けられており、例えば図示するように、USBケーブル50の一方のUSBプラグ52をプレーヤ20のUSBコネクタ32と接続し、他方のUSBプラグ51をパーソナルコンピュータ10側に設けられているUSBコネクタ（ここでは図示せず）に接続するようにされる。このようにして接続されることで、パーソナルコンピュータ10とプレーヤ20の間でデータ送受信を行って、コンテンツデータを互いに授受することが可能となる。なお、USBコネクタ32にUSBプラグ52を接続しないときには、コネクタ蓋部33によりUSBコネクタ32を覆って保護できるようになっている。

【0020】1-2.システムの利用形態

ここで、上記したシステムの利用形態例について説明しておく。図2(a)に示すようにして、パーソナルコンピュータ10ではEMDサーバ1から或るコンテンツデータCTを購入してダウンロードして取り込むようにされる。このようにして取得されたコンテンツデータCTは、パーソナルコンピュータ10において前述したように圧縮処理が施され、また、暗号化が施されたファイルに変換され、例えば内部のハードディスクに保存される。また、ここでは、図示していないが、先にも述べたように、CD等のメディアや音声入出力インターフェイスから得たオーディオデータも、コンテンツデータとして取得して保存することができる。

【0021】そして、上記のようにしてパーソナルコンピュータ10にて保存されたコンテンツデータCTは、図2(b)に示すようにして、USBインターフェイスを介して接続したプレーヤ20に対してアップロードすることが可能とされている。プレーヤ20では、このアップロードされたコンテンツデータを内蔵のフラッシュメモリに書き込んで記憶する。そして、ユーザは、プレーヤ20によりフラッシュメモリに記憶されたコンテンツとしての楽曲であるオーディオデータを再生して聴くことができる。

【0022】また、本実施の形態のシステムは、SDMI(Secure Digital Music Initiative)という著作権保護規格に準拠しているものとされる。つまり、パーソナルコンピュータ10にインストールされるコンテンツ管理アプリケーション、及びプレーヤ20は、このSDMIに準拠した動作が得られるように構成されている。

【0023】図3は、このSDMIに準拠した代表的なデータ転送制限を示している。ここで、パーソナルコンピュータ10からプレーヤ20に対してコンテンツデー

タをコピーするようにして転送することについては、「チェックアウト」という。この場合のデータ転送はコピーであり、パーソナルコンピュータ10においては、コピー元のコンテンツデータは削除されずに残ることになる。また、逆にプレーヤ20からパーソナルコンピュータ10に対してデータを転送することをチェックインという。ただし、チェックインの場合にはデータの移動となり、従って、チェックインによっては、プレーヤ20側で記憶されていたコンテンツデータは削除される。

【0024】ここで、チェックアウトは、3回までであると決められており、4回以上のチェックアウトは行えないものとされている。つまり、パーソナルコンピュータ10からは、本実施の形態のプレーヤ20を含む他の機器に対しては、3回までしかコピーを行うことができないように制限される。ただし、例えばすでに3回チェックアウトされたコンテンツデータをチェックインすれば、このチェックインされたコンテンツデータについては、再びチェックアウトすることができるようにされる。なお、確認のために述べておくと、図2及び図3により述べた、EMDサーバ1からのコンテンツデータのダウンロード、ダウンロードデータに対する圧縮処理、暗号化処理、また、プレーヤ20へのアップロード、そして、上記したチェックイン/チェックアウトの管理は、パーソナルコンピュータ10にインストールされたコンテンツ管理アプリケーションが行う。

【0025】ところで、EMDサーバ1におけるデータ配信としては、例えば配信サービスに多様性を与えることや著作権者の意図など反映することを目的として、再生可能期間や再生可能回数の制限を設けた「再生制限付」のコンテンツデータを提供することも行われている。これらの再生可能期間や再生可能回数は、例えばコンテンツデータのヘッダにおいて再生条件データとして格納されている。

【0026】本実施の形態としては、このような再生制限付きのコンテンツデータについては、パーソナルコンピュータ10上でコンテンツ管理アプリケーションを起動させることによっての再生のみが可能とされ、プレーヤ20へのチェックアウトは行えないものとして管理するようにされる。

【0027】ただし、もちろんのこと、再生制限付きのコンテンツデータCTをプレーヤ20にチェックアウトし、プレーヤ20により再生制限付きのコンテンツデータが再生可能なように構成することは可能である。そして、当然のこととして、再生制限付きのコンテンツデータCTが指定する再生可能期間や再生可能回数に従って、プレーヤ20における再生動作も制限されるように構成されるべきものである。

【0028】続いて、図1に示したシステムを構成するパーソナルコンピュータ10及びプレーヤ20の内部構成について、図4を参照して説明する。パーソナルコン

ピュータ10においては、ネットワーク2と接続するためのネットワーク接続インターフェイス101が設けられ、CPU102の制御によってネットワーク接続インターフェイス101が機能することで、ネットワーク2を介してEMDサーバ1と通信可能に接続され、EMDサーバ1にて提供されているコンテンツデータをダウンロードすることが可能なる。

【0029】また、ここではCD-ROMドライブ106が設けられており、このCD-ROMドライブ106では、装填されたCDフォーマットのディスクに記録されているデータを再生して読み込むことが可能とされる。なお、例えば実際にはCDフォーマットのディスクに加えて、DVD(Digital Versatile Disc)などのディスクも再生可能なディスクドライブが設けられてもよい。例えば、コンテンツデータとしては、このCD-ROMドライブ106に装填されたディスクを再生して得たオーディオデータを利用することができる。

【0030】また、音声入出力インターフェイス108は、外部機器とのデジタルオーディオ信号、もしくはアナログオーディオ信号の入出力のためのインターフェイスとされる。本実施の形態のパーソナルコンピュータ10では、この音声入出力インターフェイス108を介して入力されるデジタルオーディオ信号及びアナログオーディオ信号をコンテンツデータに変換することも可能とされる。

【0031】ハードディスク107には、CPU102が実行するための各種アプリケーションソフトウェアや、各種ファイルが保存される。例えば本実施の形態の場合であれば、コンテンツ管理アプリケーションと、このコンテンツ管理アプリケーションが扱うコンテンツデータのファイルがここに保存される。

【0032】RTC105は、現在時刻を計時してその時刻情報を出力する。このRTC105にて得られる現在時刻情報は、本実施の形態においては、コンテンツデータの再生期限管理などに用いることができる。

【0033】インターフェイス10は、例えば実際にはマウス、キーボード等とされる操作入力部112から入力される操作情報をCPU102に伝送し、また、画像をディスプレイ113に表示させるためのユーザインターフェイス機能を有している。また、外部周辺機器とのデータインターフェイス機能も有しているものとされる。そして、本実施の形態としては、少なくとも、USBインターフェイスによって外部周辺機器との通信が可能のようにされており、従って、インターフェイス10においては、USBインターフェイスによるデータ通信を実現するためにUSBドライバ110が設けられる。USBドライバ110は、例えば実際にはパーソナルコンピュータ10本体に出出して設けられるUSBコネクタ111と接続される。本実施の形態の場合であれば、USBインターフェイスによってプレーヤ20と接続さ

れた場合には、コンテンツ管理アプリケーションのプログラムに従って、プレーヤ20に対して楽曲としてのコンテンツデータを転送することができる。つまり、CPU102の制御によって、コンテンツデータがUSBドライバ110に転送され、USBドライバ110では、USBコネクタ111を介してコンテンツデータを送信出力する。

【0034】ここで、パーソナルコンピュータ10側のUSBコネクタ111と、プレーヤ20側のUSBコネクタ32とを接続するUSBケーブル50としても示されるように、USBインターフェイスとしては、信号ラインD+、D-、電源ラインVbus、GNDラインの4本のラインで1本のケーブル（伝送路）を形成する。信号ラインD+、D-は、差分伝送によりデータ伝送を行うデータ用ラインであり、電源ラインVbusは、パーソナルコンピュータ10から電源供給を行うためのプラス側のラインとされる。つまり、周知のように、USBインターフェイスでは、例えばパーソナルコンピュータ10から周辺機器に対して直流電源供給を行うことが可能とされている。

【0035】CPU（Central Processing Unit）102は、パーソナルコンピュータ10内において、例えばOS（Operation System）としてのプログラムや、起動された各種アプリケーションソフトウェアのプログラムに従って所要の制御処理を実行する。ROM113は、例えばEEPROMやフラッシュメモリなどの不揮発性メモリとされて、各種設定情報や、さほどのデータ容量を有さないファイルなどのデータを適宜保存しておくことが可能とされる。RAM104には、例えば起動されたアプリケーションソフトウェアのプログラムデータや、CPU102の処理によって得られる各種データが保持される。

【0036】電源部114は、例えば実際には商用交流電源を入力して、所定レベルの直流電源電圧を得る。そして、このようにして得られた電源PWを、内部の各機能回路部に対して供給する。また、前述したようにして、USBインターフェイスを介して当該パーソナルコンピュータ10から外部周辺機器に対して電源供給を行うために、上記電源部114からは、USB用電源PWuを、USBドライバ110に対して分岐して供給するようにもされている。

【0037】続いて、上記構成によるパーソナルコンピュータ10において起動されるコンテンツ管理アプリケーションとしての機能を、図5に模式的に示す。コンテンツ管理アプリケーション300は、大きくは、コンテンツ管理プログラム311、表示操作指示プログラム312、録音プログラム313、購入用アプリケーションプログラム315から成り、また、コンテンツデータベース314を作成して用意する。なお、コンテンツデータベース314は、例えばハードディスク107に保存

される。

【0038】コンテンツ管理プログラム311は、例えば、実際にはシャッフルされたインストラクション、または暗号化されたインストラクションなどとして記述されることで、その処理内容を外部から隠蔽して、その処理内容の読解が困難となるようにされている。

【0039】このコンテンツ管理プログラム311において、EMD選択プログラム131は、例えばユーザの所定操作によって行われるEMD登録処理によって、ネットワーク2を介してEMDサーバ1側から提供されるプログラムである。そして、このEMD選択プログラム131を例えばRAM104に格納して保持するようにされる。そして、EMD選択プログラム331は、例えば実際には複数あるとされるEMDサーバ1のうちの何れと接続するのかについての選択を行い、この選択されたEMDサーバ1との接続を、購入用アプリケーションプログラム315、または購入用ドライバ342に実行させる。

【0040】チェックイン／チェックアウト管理プログラム332は、コンテンツデータのチェックイン／チェックアウトの動作を管理するもので、指定されたコンテンツデータについてチェックアウトが許可されていればチェックアウトを行い、また、チェックインが要求されたコンテンツについて許可が与えられているのであれば、チェックインが行われるように処理を実行する。このチェックイン、チェックアウトが許可されているか否かについての判定は、例えば、図3にて説明したチェックイン／チェックアウトの規則、およびコンテンツデータベース314において、チェックイン／チェックアウトの対象となったコンテンツデータに対応するデータ内容をチェックすることで行われる。また、チェックイン／チェックアウト管理プログラム332は、チェックイン又はチェックアウトの処理に対応して、コンテンツデータベース314の内容を更新する。なお、コンテンツデータベース314の構造については後述する。

【0041】また、ネットワーク2を介して購入用アプリケーションプログラム315がEMDサーバ1から受信したコンテンツデータは、例えば、このコンテンツ管理アプリケーション300において実行するデータの暗号化方式とは異なる方式によって暗号化されている場合がある。暗号方式変換プログラム333は、上記のようにしてEMDサーバ1から受信して取得したコンテンツデータの暗号化方式について、このコンテンツ管理アプリケーション300が適合する暗号化方式によって暗号化されたデータ形式に変換する。この場合のコンテンツデータに対する暗号化方式としては、例えばDES（Data Encryption Standard）方式、又はFEAL（Fast Encryption Algorithm）方式などを採用することができる。

【0042】さらに、EMDサーバ1から受信して取得したコンテンツデータとしては、コンテンツ管理アプリ

10

20

30

40

50

ケーション300が対応するATRAC3方式とは異なる圧縮方式（例えば、MP3：MPEG Audio Layer-3など）によってオーディオデータの圧縮が施されている場合もあるので、このような場合には、圧縮方式変換プログラム334によって、ATRAC3方式以外の方式によって圧縮されているコンテンツデータとしてのオーディオデータについて、ATRAC3方式により圧縮されたオーディオデータへの変換を行うようにされる。また、圧縮方式変換プログラム334は、圧縮処理が施されていないオーディオデータを圧縮処理するエンコーダとしての機能も有しており、例えばCD-ROMドライブ106によりディスクから再生されたオーディオデータや、音声入出力インターフェイス108により入力して取得したオーディオデータについてATRAC3方式による圧縮処理を施すことも行うようにされる。

【0043】暗号化プログラム335は、例えばCD-ROMドライブ106によりディスクから再生されたオーディオデータや、音声入出力インターフェイス108により入力して取得したオーディオデータをコンテンツデータとして作成する際に、コンテンツ管理アプリケーション300が適合する暗号化方式によって暗号化を施す。

【0044】ここで、上記しているコンテンツ管理アプリケーション300に適合する暗号化方式、及びオーディオデータ圧縮方式は、正規のプレーヤ20も対応しているものとされる。つまり、プレーヤ20においては、コンテンツ管理アプリケーション300により適正に圧縮処理及び暗号化が施されたコンテンツデータについては、伸長処理及び暗号複合化処理を実行してオーディオデータを復元し、適正に再生することが可能とされている。

【0045】利用条件変換プログラム336は、EMDサーバ1から受信して取得したコンテンツデータの再生条件、コピー条件等を示す利用条件データ（Usage Rule）のフォーマットを、「コンテンツ管理アプリケーション300により処理可能なフォーマットに変換する。この利用条件データは、コンテンツデータベースを作成するのに使用される。

【0046】ハッシュ値管理プログラム337は、先ず、後述するデータ構造を有するコンテンツデータベース314についてのハッシュ値を算出して、これを例えばROM105に対して格納する処理を実行する。また、チェックインまたはチェックアウトの処理を実行する前段階においてハッシュ値を参照することで、コンテンツデータベース内の利用条件データの改竄を検出する。また、例えば改竄が行われないとして、この後に或るコンテンツデータについてのチェックインまたはチェックアウトの処理が実行された場合には、ハッシュ値を更新することも行う。ハッシュ値は、データに対してハッシュ関数を適用して演算を行うことで得られるもので

ある。ハッシュ関数は、可変長の長いデータを固定長の短い値にマッピングするようにして変換する一方方向性の関数として知られており、演算結果であるハッシュ値同士の間には衝突は起こりにくいとされている。

【0047】また、実際にパーソナルコンピュータ10とプレーヤ20がUSBインターフェイスにより接続された場合には、例えばコンテンツデータの授受を行う前段階において、パーソナルコンピュータ10にインストールされているコンテンツ管理アプリケーションが正規のものであるか否かを確認する共に、プレーヤ20が正規のものであるか否かを確認するために、パーソナルコンピュータ10とプレーヤ20との間で相互認証処理を実行する。認証プログラム338は、この相互認証処理にあたって、パーソナルコンピュータ10側が実行すべき認証処理を実行するプログラムとされる。また、コンテンツ管理プログラム311と購入用アプリケーションプログラム315との相互認証処理、コンテンツ管理プログラム311と購入用ドライブ342との相互認証の処理を実行する。さらにはEMDサーバ1と購入用アプリケーションプログラム315又は購入用ドライブ342との相互認証処理を実行し、このときに利用される認証鍵を例えばROM103に記憶させる。なお、この認証鍵は、コンテンツ管理プログラム311がパーソナルコンピュータ1にインストールされたときには、認証プログラム338に記憶されてはいないものとされる。そして、表示操作指示プログラム312により登録処理が正常に実行されたとき、EMDサーバ1から供給される。

【0048】復号プログラム339は、このコンテンツ管理アプリケーション300上でコンテンツデータを再生するとき、そのコンテンツファイルについて所要の復号処理を施して、オーディオデータに復元することを行う。例えば、コンテンツデータが既に圧縮処理が施され、また暗号化が施されているのであれば、暗号化を解き、また伸長処理を行うことで、オーディオデータを得る。このようにして得られたオーディオデータは、例えば音声入出力インターフェイス108を介して出力される。

【0049】電源制御プログラム340は、後述するようにして、USBドライブ110における電源制御を実行するために設けられる。

【0050】デバイスドライバ341は、例えばプレーヤ20としてのデバイスに対応するドライバソフトウェアであり、USBドライブ110を介してのプレーヤ20とのデータ送受信を司る。

【0051】購入用ドライブ342は、例えば或る特定のEMDサーバに対応したドライバソフトウェアであり、コンテンツ管理アプリケーション300本体に対していわゆるプラグインソフトウェアとしてインストールされる。これにより、購入用ドライブ342は、コンテ

10

20

30

40

50

ンツ管理プログラム311とのデータの授受が可能となる。そして、この購入用ドライバ342は、ネットワーク2を介して或る特定のEMDサーバ1に所定のコンテンツデータの送信を要求するとともに、このEMDサーバ1からコンテンツデータを受信する。また、購入用ドライバ342は、このEMDサーバ1からコンテンツデータを受信するとき、課金処理も実行するようにされる。

【0052】GUI(Graphical User Interface)プログラム312は、コンテンツ管理アプリケーション300としてのGUIを実現するためのプログラムとされ、例えば操作入力部112としてのマウス、キーボード等の操作に応じて、ディスプレイ113に対してGUI画像の表示を行う。

【0053】録音プログラム313は、例えばGUIプログラム312により録音用ウィンドウが表示されている状態のもとで、例えば現在選択されているCD-ROMドライブ106に装填されているCDのオーディオデータ、又は音声入出力インターフェイス108を介して取得されるオーディオデータを音源として、ハードディスク107にコンテンツデータとして保存するための処理を実行するプログラムとされる。例えば、録音用ウィンドウに対して録音開始の操作が行われると、録音プログラム313は、現在、選択されている音源としてのオーディオデータを、例えばコンテンツデータの形式によりハードディスクに保存する。

【0054】コンテンツデータベース314は、例えば、ファイルとして管理されてハードディスク107に保存されているコンテンツデータごとに対応した所要の管理情報ファイルの集合から成る。そして、このコンテンツデータベース314も例えばファイルとして、ハードディスク107に対して保存されているものとされる。

【0055】ここで、上記コンテンツデータとコンテンツデータベース314のデータ構造例について、それぞれ図8、図9を参照して説明する。図8はコンテンツデータの構造を示している。コンテンツデータとしては、図示するように先ずヘッダエリアA1が配置され、これに続けてオーディオデータが格納されるデータエリアA2が配置される。なお、これまでの説明からも分かるように、データエリアA2に格納されるオーディオデータは、ATrac3方式により圧縮処理が施されており、また、例えばDESなどの所定方式によって暗号化されている。

【0056】ヘッダエリアA1には、先頭から、ファイルID、ヘッダサイズ、コンテンツキー、ファイルサイズ、コーデックID、ファイル名、ファイル情報、再生制限データ、再生開始日、再生終了日、再生可能回数、実再生回数の各情報が格納される。

【0057】ファイルIDは、ファイルごとに固有とな

るIDであり、ヘッダサイズは、ヘッダエリアA1のサイズを示す。コンテンツキーは、暗号化が施されたデータエリアA2のオーディオデータについて暗号化を解くためのデータとされ、実際にパーソナルコンピュータ10とプレーヤ20との間でコンテンツデータの授受が行われる際に、共通のセッションキーでさらに暗号化される。

【0058】ファイルサイズは、例えばこのコンテンツデータ自体のファイルとしてのサイズを示し、ファイル情報には、例えばこのコンテンツデータの楽曲としてのタイトルや、アーティスト名を示す。

【0059】コーデックIDは、コンテンツデータとしてのオーディオデータに対して施されている音声圧縮方式を示すIDとされる。

【0060】再生制限データ、再生開始日、再生終了日、再生可能回数、実再生回数は、当該コンテンツデータの再生制限が適正に行われるようにするための再生制限管理情報である。再生制限データは、例えばSDMIの規則に従ったうえで、これまでのデータ転送や再生履歴に応じて設定される再生制限を示す情報とされ、例えば後述するコンテンツデータベースのコピー条件やコピー回数カウンタの値などが反映される。また、再生開始日時及び再生終了日時は、再生期間に制限が与えられた再生制限付きのコンテンツデータである場合に、その再生が可能とされる開始日時と終了日時を示す。同様に、再生可能回数は、再生回数が制限される再生制限付きのコンテンツデータについて、その再生可能回数の値を示す。実再生回数は、パーソナルコンピュータ10あるいはプレーヤ20により再生された回数を示す。ここで、例えば実再生回数か示す値が、再生可能回数の値と同一となった場合には、パーソナルコンピュータ10及びプレーヤ20では、このコンテンツデータの再生を禁止することになる。

【0061】図9は、コンテンツデータベースの構造を示している。ここでは、コンテンツデータとして、コンテンツ1～3の3つがハードディスク107に保存されている場合に対応しているものとされる。

【0062】この図に示すように、各コンテンツに対応しては、先ず、ファイルID、コンテンツキー、タイトル、ファイルサイズの情報が設けられ、さらに利用条件データが設けられる。ファイルID、コンテンツキー、タイトル、ファイルサイズは、上記図8に示したコンテンツデータのヘッダエリアA1に格納されているものと、同じ内容を示すものとされる。

【0063】また利用条件データのうち、「再生条件：開始日時」、「再生条件：終了日時」、「再生条件：再生可能回数」も、図8に示したコンテンツデータのヘッダエリアA1に格納されている再生開始日時、再生終了日時、再生可能回数と同じ内容を示す。また、「再生回数カウンタ」は、図8に示したコンテンツデータのヘッ

ダエリア A 1 に格納されている実再生回数と同じ内容を示す。「再生時課金条件」は、当該コンテンツデータについての課金設定条件が示される。「コピー条件：回数」は、当該コンテンツデータについて許可されているコピー回数を示し、本実施の形態の場合であればチェックアウトの回数＝3 が示されることになる。「コピー回数カウンタ」は、これまでに、当該コンテンツデータがコピーされた回数を示す。例えば上記「コピー条件：回数」で示される値と、「コピー回数カウンタ」の値が同じになれば、これ以上、このコンテンツデータをコピーすることが禁止される。つまり、例えばパーソナルコンピュータ 10 では、このコンテンツデータのコピー要求があってもこれには応じない。なお、このコピー回数カウンタの値は、チェックインが行われた場合には、コピー回数を 1 回分少なくするようにしてその値が変更される。「コピー条件：SCMS」には、SCMS (Serial Copy Management System) の規格に基づくコピー条件が示される。SCMS では、例えば或るコピー元のメディアからコピー先のメディアに対してオーディオデータ等のデジタルコピーを行うのについて、1 世代のみのコピーを許可している。また、ハッシュ値は所定バイト数から成るデータ列であり、前述したハッシュ値管理プログラム 337 (図 5 参照) がコンテンツデータベースの内容に基づいて算出して保持しておくようにされ、コンテンツデータベース内容についての改竄が行われたか否かについての判定を行う場合に参照される。

【0064】続いて、説明を図 4 に戻して、プレーヤ 20 の内部構成について説明する。プレーヤ 20 には、図 1 にも示した USB コネクタ 32 が設けられ、この USB コネクタ 32 は、内部の USB ドライバ 215 と接続されている。本実施の形態の場合、パーソナルコンピュータ 10 から送信されたコンテンツデータは、上記 USB コネクタ 32 から USB ドライバ 215 に入力されて、ここで受信される。

【0065】フラッシュメモリ 206 は、フラッシュメモリドライバ 205 によって、データの書き出し及び読み出しが行われる。そして、この場合には、USB ドライバ 215 にて受信されたコンテンツデータをフラッシュメモリ 206 に対して書き込んで記憶する。

【0066】ここで、フラッシュメモリ 206 に記憶されるコンテンツデータは、いわゆる FAT (File Allocation Table) によって管理される。つまり、FAT によって、フラッシュメモリ 206 上におけるコンテンツデータの記録位置が管理される。なお、この FAT としてのデータは、例えばコンテンツデータと共にフラッシュメモリ 206 に記憶されてもよいのであるが、例えば EEPROM などによって構成される外部 ROM 210 に記憶するようにしてもよい。例えば外部 ROM 210 に FAT を書き込むようにすれば、その構造上、書き換え回数に限度があるとされているフラッシュメモリ 206

に対する書き換え回数を少なくすることができる。また、外部 ROM 210 には、例えば各種設定情報なども記憶しておくのに利用することができる。

【0067】フラッシュメモリ 206 に記憶されたコンテンツデータをオーディオデータとして再生する際には、先ず、指定されたコンテンツデータをフラッシュメモリ 205 から読み出して、内部バスを介して DSP 207 に転送する。DSP 207 においては、コンテンツデータからデータエリア A 2 に格納されているオーディオデータを抜き出す。そしてこのオーディオデータについて、暗号化の解読処理、及びデータ伸長処理を実行し、所定フォーマットのデジタルオーディオデータを得る。また、例えば操作部 212 に対して行われた所定操作に応じた音質、音量等の調整も、この DSP 207 における信号処理によって行うことができる。なお、DSP 207 が信号処理を行うのにあたっては、例えば必要があればバッファメモリ 211 を作業領域として利用するようにされる。そして、このようにして得られたデジタルオーディオデータを D/A コンバータ 208 に出力する。D/A コンバータ 208 では、入力されたデジタルオーディオデータをアナログオーディオ信号に変換してアンプ 209 に対して出力する。アンプ 209 では入力されたアナログオーディオ信号について増幅を行って、音声信号出力端子であるヘッドフォンジャック 22 に出力する。そして、ヘッドフォンジャック 22 にヘッドフォン 40 が接続されれば、このヘッドフォン 40 のイヤドライバ 42 から、例えば楽曲としての音声が出力される。

【0068】また、フラッシュメモリ 206 に記憶されたコンテンツデータをチェックインする、つまり、パーソナルコンピュータ 10 に対して移動させるようにして転送する際には、フラッシュメモリドライバ 205 により、チェックインすべきコンテンツデータをフラッシュメモリ 205 から読み出して、USB ドライバ 215 に転送する。USB ドライバ 215 では、USB コネクタ 32 → USB ケーブル 50 を介して接続されているパーソナルコンピュータ 10 側の USB ドライバ 110 に対して、コンテンツデータを送信出力する。

【0069】また、先にも述べたように、パーソナルコンピュータ 10 とプレーヤ 20 が USB インターフェイスにより接続された場合には、パーソナルコンピュータ 10 とプレーヤ 20 間で相互認証を行うのであるが、このために、プレーヤ 20 側においては、認証処理ブロック 204 が設けられる。認証処理ブロック 204 は、例えば CPU 201 の制御に応じて、相互認証処理としてプレーヤ 20 側が行うべき処理を実行する。

【0070】操作部 212 は、例えば図 1 に示したプレーヤ 20 の本体 21 に設けられる各種操作子より成るものとされ、操作子に行われた操作に応じた操作情報信号を出力する。CPU 201 は、この操作情報信号に基づ

10

20

30

40

50

いて、各種機能回路部に対する制御処理を実行する。これにより、操作に応じた所要の動作が得られる。例えば再生に関する操作が行われたのであれば、この操作に応じて所要の再生関連動作が行われるように、DSP207に対する制御やフラッシュメモリ205に対する読み出し制御等を実行する。また、表示ドライバ213は、CPU201から出力される表示データに応じて、表示部30としての表示デバイスに対する駆動を行う。これにより、表示部30において、各種の表示が行われる。

【0071】CPU216は、上記した操作部に応じたコンテンツデータに対する各種再生処理、表示制御、USBインターフェイスを介しての通信制御をはじめ、所要の動作を実現するための各種制御処理を実行する。ROM202には、CPU201が実行すべきプログラムのデータや、CPU202が参照すべき初期設定情報などが格納される。また、RAM203には、CPU201が実行すべきプログラムが起動されて保持されると共に、CPU201が各種処理や演算に利用したデータが保持される。

【0072】本実施の形態のプレーヤ20は、バッテリー217にて得られる直流電源を電源回路216によって所定レベルの電圧に変換して、内部回路の電源PW・Bとして利用するようにされている。また、前述したように、パーソナルコンピュータ10からはUSBケーブル50を介して直流電源電圧を外部に供給することが可能とされている。このため、プレーヤ20としては、USBケーブル50を介してパーソナルコンピュータ10と接続されているときには、このUSBケーブル50を介して供給される電源電圧を内部回路に供給するようにされる。このために、本実施の形態のUSBドライバ215としては、USBケーブル50を介して供給される電源電圧から所定レベルの電源PW・Uを得て、これを内部回路に供給するように構成される。このとき、バッテリー217を電力源とする電源回路216からの電源供給は停止されるのであるが、この電力源切り換えの構成については、次の説明において述べていくこととする。

【0073】本実施の形態のシステムでは、後述するようにして、パーソナルコンピュータ10とプレーヤ20との間で行った相互認証結果に応じて、USBインターフェイスを介しての電源（USB電源）の供給を制御するようにされる。つまり、パーソナルコンピュータ10とプレーヤ20との相互認証結果として、プレーヤ20が正規のシステム対応機器ではないとして認証されなかった場合には、ペナルティ的な措置として、例えば1つには、パーソナルコンピュータ10からプレーヤ20へのUSB電源の供給を停止させるものである。

【0074】そこで、上記図2に示したパーソナルコンピュータ10とプレーヤ20の電源回路系の構成例を図6及び図7に示しておくこととする。図6は、パーソナルコンピュータ10における電源回路系として、USB

電源の供給回路系の構成を示している。USBドライバ110に対しては、電源部114から、USB用電源PWuがUSBドライバ110に対して供給される。ここでは、USBドライバ110内において、電源経路内にスイッチ110aが設けられているものとされ、上記USB用電源PWuは、このスイッチ110aからラインVbusを介してUSBコネクタ111に接続されるようになっている。ここで、スイッチ110aは、例えばFETなどのスイッチ素子が用いられ、CPU102の制御によってオン／オフ状態が制御される。

【0075】また、図7にプレーヤ20側に設けられる電源回路系の構成を示す。プレーヤ20では、バッテリー217とUSB電源の何れかを電力源として動作することが可能とされている。まず、USBコネクタ32を介してパーソナルコンピュータ10などの外部機器と接続されていない状態では、バッテリー217を電力源とすることになる。この場合、バッテリー216から供給される直流電源電圧としての電力は電源回路215に供給され、この電源回路215内のDC／DCコンバータ215aにて所定レベルで安定化された直流電圧に変換されて、電源PW・Bとして例えばCPU201等をはじめとする所要の回路素子に対して供給される。また、このときには、USBコネクタ32→レギュレータ216aを介してのUSB電源側からの電源供給は無い。

【0076】そして、例えば上記した状態から、プレーヤ20のUSBコネクタ32を介してパーソナルコンピュータ10などの外部電源供給機器との接続が行われたとする。このとき、USBコネクタ32を介しては、信号ラインD+、D-によるデータ信号と、電源ラインVbusによるUSB電源とが入力されてくることになるが、ここでは、説明の都合上、USB電源を供給する電源ラインVbusのみを示している。

【0077】USBコネクタ32を介して入力されたUSB電源は、USB検出信号生成部220及びUSBドライバ216内に対して設けられているとされるレギュレータ216aに対して供給される。USB検出信号生成部220では、入力されたUSB電源の電圧を分圧して、USB接続が行われたことを示し得る検出信号を生成して、電源回路215内のDC／DCコンバータ215aに対して出力する。DC／DCコンバータ215aは、この検出信号が入力されると、その動作を停止させるようにされている。つまり、USB接続が行われた場合には、DC／DCコンバータ215aの動作を停止させるように制御することで、バッテリー216を電力源とする電源供給は行わないようにされる。そして、これに代わって、レギュレータ216aにより入力されたUSB電源を所定レベル電圧に変換して得られる電源PW・Uを内部回路に対して供給するようにされている。

【0078】ここで、例えば上記した状態からUSB接続が外された状態となったとすれば、レギュレータ21

10

20

30

40

50

6aを介しての電源PW・Uの供給が停止される代わりに、DC/DCコンバータ215aが動作を開始するようにされ、再びバッテリー駆動される状態に切り換えられる。

#### 【0079】5. データ転送処理

##### 5-1. チェックアウト処理

本実施の形態としては、上記してもいるように、相互認証処理結果に応じたUSB電源制御に特徴を有するのであるが、相互認証処理は、パーソナルコンピュータ10とプレーヤ20間とでのデータ転送を行う際に、互いが正規のものであるのかを確認するために実行されるものである。そこで次に、この相互認証処理を含むデータ転送時の処理動作について説明を行っていく。本実施の形態のデータ転送としては、前述したように「チェックアウト」といわれるパーソナルコンピュータ10からプレーヤ20へのデータコピーと、「チェックイン」といわれるプレーヤ20からパーソナルコンピュータ10へのデータ移動（ムーブ）が行われることから、このチェックアウト処理とチェックイン処理について順次説明していく。

【0080】図10及び図11には、チェックアウトのための処理動作が示されている。この図に示すフローチャートは、パーソナルコンピュータ10側からみた場合の処理を示しており、コンテンツ管理アプリケーションのプログラムに従ってCPU102が実行するものとされる。

【0081】チェックアウトに際しては、先ず図10のステップS101において、現在のコンテンツデータベース全体の内容に対応するハッシュ値を計算する。そして、次のステップS102において、上記ステップS101にて得られたハッシュ値と、前回において算出されて例えばROM103に保持させておいたハッシュ値とについて比較を行って、その値が一致しているか否かについて判別する。ここで、両者のハッシュ値が一致していないとして否定結果が得られた場合には、ステップS103に進んで、コンテンツデータベースが不正に改竄された可能性があるためにチェックアウトを行わない旨を示すメッセージを表示させ、このルーチンを終了させる。これに対してステップS103において両者のハッシュ値が一致しているとして肯定結果が得られた場合にはステップS104に進む。

【0082】ステップS104においては、例えばハードディスク107に保存されているコンテンツデータベースから、そこに登録されている各コンテンツの情報を読み出す。そしてこの読み出した情報に基づいて、ディスプレイ113に対して、コンテンツデータ（即ち楽曲である）の選択を行うためのGUI画像を表示させるための制御処理を実行する。ユーザは、例えば操作入力部12を用いて、このコンテンツ選択のためのGUI画像に対して操作を行うことで、チェックアウトすべきコン

テンツを選択することができる。

【0083】ここで、例えば上記ステップS105において行われたとされるユーザ操作によって、チェックアウトすべきコンテンツデータの決定が行われたとすると、続くステップS105において、コンテンツデータベース内において、この選択されたコンテンツデータに対応する利用条件データをチェックする。つまり、選択されたコンテンツデータについての各種再生条件、コピー条件、再生時課金条件などを調べる。そして、次のステップS106において、例えば上記した各利用条件データのチェック結果に基づいて、選択されたコンテンツについてチェックアウトが可能であるか否かについて判別する。ここで、チェックアウトが禁止されるべきものであるとして判別された場合にはこのルーチンを終了するが、チェックアウトが可能である場合には、ステップS107に進む。

【0084】続くステップS107においては、パーソナルコンピュータ10のプレーヤ20との間での相互認証処理を実行する。

【0085】この相互認証処理の詳細については後述するが、ここで簡単に説明しておく、例えば、プレーヤ20の外部ROM210にはマスター鍵KMが予め記憶され、パーソナルコンピュータ10のROM103には個別鍵KI、及び当該パーソナルコンピュータ10としての機器を特定するIDが予め記憶されているものとする。プレーヤ20側では、パーソナルコンピュータ10側から送信されるIDの受信し、そのIDとプレーヤ20側で保持するマスター鍵KMにハッシュ関数を適用して、パーソナルコンピュータ10側のROM103に保持しているとされる個別鍵と同一の鍵を生成する。このようにすることで、パーソナルコンピュータ10とプレーヤ20の両方に、共通の個別鍵が共有されることになる。この個別鍵を用いてさらに、一時的な通信用鍵を生成することができる。

【0086】あるいは他の認証処理としては、例えばパーソナルコンピュータ10のROM103にIDとマスター鍵KM1を予め記憶させておくとともに、プレーヤ20の外部ROM210にもプレーヤ20のIDとマスター鍵KM2を記憶させておくようにする。そして、それぞれのIDとマスター鍵をお互いに他方に送信することで、他方は一方から送信されてきたIDとマスター鍵にハッシュ関数を適用して、他方の個別鍵を生成する。そして、その個別鍵から、一時的な通信用鍵をさらに生成するようにしてもよい。

【0087】そして、上記ステップS107において、例えば相互に認証が得られたとされる場合には、最終的には、上記した一時的な通信用鍵（一時鍵Ks）をパーソナルコンピュータ10のプレーヤ20とで共有したうえで、ステップS108に移行する。なお、相互認証が得られなかった場合の処理については、後述する。

【0088】ステップS108においては、ファイルIDなどのコンテンツデータとしてのファイルが特定できる情報をコンテンツデータベースから読み出す。そして、次のステップS109において、必要があれば、上記ステップS108により取得したコンテンツデータに含まれるオーディオデータの圧縮符号化方式及び暗号化方式、フォーマットなどをプレーヤ20に対応するものに変換する処理を実行する。ただし、ハードディスク107に保存されていた段階で、プレーヤ20に対応する圧縮符号化方式及び暗号化方式、フォーマットとされているのであれば、この処理はスキップされる。このステップS109の処理が終了すると図11のステップS110の処理に移行する。

【0089】ステップS110においては、ハードディスク107から読み出して取得したコンテンツデータを、先のステップS107の相互認証処理により共有した通信用鍵（一時鍵）で暗号化する。そして、プレーヤ20に対してUSBインターフェイスを介して転送する。プレーヤ20側では、上記のようにして転送されてきたコンテンツデータを受信してフラッシュメモリ206に書き込んで記憶させる。

【0090】次のステップS111においては、必要があれば、選択されたコンテンツデータに対応するコンテンツデータベースの各再生条件（開始日時、終了日時、再生可能回数）を、プレーヤ20が管理可能な形式に変換する。さらに続くステップS112において、選択されたコンテンツデータに対応するコンテンツデータベースのコピー条件中のSCMS情報を、プレーヤ20の管理する形式に変換する。そして、次のステップS113において、上記ステップS111、S112の処理によって変換された再生条件とSCMS情報を、プレーヤ20に転送する。プレーヤ20側では、受信した再生条件とSCMS情報を、フラッシュメモリ206、もしくは外部ROM210に対して保存する。

【0091】また、次のステップS114においては、選択されたコンテンツのコンテンツデータベース中に登録されている利用条件データである、各種再生条件、再生時課金条件、コピー条件などを、CPU102が扱っている形式のまま、プレーヤ20に転送する。プレーヤ20側では、転送されてきた利用条件データを例えばフラッシュメモリ206、もしくは外部ROM210に対して保存することになる。

【0092】次のステップS115においては、選択されたコンテンツデータを暗号化している暗号鍵、即ちコンテンツキーをコンテンツデータベースから読み出し、ステップS116において、そのコンテンツキーをROM103に記憶されている保存用鍵で復号し、通信用鍵で暗号化する。そして、通信用鍵で暗号化したこのコンテンツキーを、プレーヤ20に転送する。プレーヤ20側では、CPU201が制御する認証処理ブロック20

4の処理によって、パーソナルコンピュータ10から転送されてきた暗号鍵を相互認証処理で共有した通信用鍵を用いて復号し、自分自身の保存用鍵を用いて暗号化する。そして、既に保存したデータと関連付けてフラッシュメモリ206、もしくは外部ROM210に対して保存する。このようにして、コンテンツデータ及び利用条件データなどのヘッダの情報を順次、パーソナルコンピュータ10からプレーヤ20に対して転送し、これをプレーヤ20側にて受信、記憶することで、チェックアウトとしてのデータ転送が行われるものである。

【0093】そして、次のステップS117においては、パーソナルコンピュータ10側において、転送したコンテンツデータに対応するコンテンツデータベースのコピー回数カウンタを1つインクリメントする。上記ステップS117の処理によって、コンテンツデータベースの内容はこれまでとは異なるものとなる。そこで、次のステップS118において、コンテンツデータベース全体のハッシュ値についての演算を行い、この新たに得られたハッシュ値をROM103に保持する。つまり、ハッシュ値の更新処理を実行するものである。

【0094】5-2. チェックイン処理  
続いて、チェックインのための処理動作について、図12のフローチャートを参照して説明する。なお、この図においては、パーソナルコンピュータ10側の処理とプレーヤ20側の処理とを1つのフローにより示している。パーソナルコンピュータ10側の処理は、コンテンツ管理アプリケーションのプログラムに従ってCPU102が実行し、プレーヤ20側の処理は、CPU201が実行する。

【0095】この図に示す処理においては、先ず、ステップS201において、パーソナルコンピュータ10からプレーヤ20に対して、プレーヤ20のフラッシュメモリ206に記憶されているコンテンツデータについての管理情報の読み出しを要求する。ここでいう管理情報とは、例えばコンテンツデータのヘッダに格納されている内容やFATなどの情報から成り、フラッシュメモリ206に記憶されているコンテンツデータについての記録再生管理に利用される情報とされる。そしてこの管理情報は、例えば外部ROM210又はフラッシュメモリ206において保存されている、この要求に応じて、プレーヤ20のCPU201は、記憶している管理情報を読み出してパーソナルコンピュータ10に送信するための制御処理を実行する。また、パーソナルコンピュータ10側では、受信した管理情報に基づいて、プレーヤ20側で記憶されている楽曲としてのコンテンツデータを選択するためのGUI画像をディスプレイ113に表示させる。ユーザは、このGUI画像に対して操作を行うことで、チェックインさせるべきコンテンツデータを選択することができる。

【0096】そして、上記ステップS201においてチ

10

20

30

40

50

チェックインさせるべきコンテンツデータの決定が行われたとすると、続くステップ S 202 としての処理により、パーソナルコンピュータ 10 側とプレーヤ 20 側との相互認証処理を実行する。この処理は、先に図 10 に示したステップ S 107 の処理と同様とされる。

【0097】続く、ステップ S 203 においては、フラッシュメモリ 206 に記憶されているコンテンツデータのうちから、チェックインのために選択指定されたコンテンツデータについての読み出しを行い、パーソナルコンピュータ 10 に転送する。パーソナルコンピュータ 10 側では、続くステップ S 204 の処理によって、プレーヤ 20 から転送されてきたコンテンツデータに対してファイル名を与え、ファイルとしてハードディスク 107 に保存する。

【0098】次にプレーヤ 20 側では、ステップ S 205 の処理によって、今回チェックインを行うべきコンテンツデータを暗号化している暗号鍵についての読み出しを行う。この暗号鍵は、例えば、先に図 10 に示したステップ S 116 の処理に応じて、プレーヤ 20 側がフラッシュメモリ 206 に保存していたものである。そしてプレーヤ 20 側では、読み出しを行った暗号鍵を自分自身に有している保存用鍵を利用して復号し、さらに通信用鍵で暗号化した後、パーソナルコンピュータ 10 に送信出力する。

【0099】パーソナルコンピュータ 10 では、ステップ S 206 の処理によって、上記ステップ S 205 によりプレーヤ 20 から送信された暗号鍵を受信し、この受信した暗号鍵を通信用鍵で復号し、さらに自分自身に有する保存用鍵で暗号化する。そしてパーソナルコンピュータ 10 は、次のステップ S 207 において、先のステップ S 204 で保存したコンテンツデータのファイル名のほか、例えばユーザが GUI 操作によって入力したとされるタイトル、アーティスト名等のファイル情報、上記ステップ S 206 で暗号化した暗号鍵などを、現在保持しているコンテンツデータベースに登録する。そして続くステップ S 208 において、コンテンツデータベース全体のハッシュ値についての更新を行う。つまり、上記ステップ S 207 の処理によってその内容が書き換えられたコンテンツデータベースに対応するハッシュ値を算出し、例えば ROM 103 に記憶させる。

【0100】また、パーソナルコンピュータ 10 側では、次のステップ S 209 において、プレーヤ 20 に対して暗号鍵の保存を行ったことの通知を行うと共に、今回チェックインさせたコンテンツデータの削除を要求する。そして、プレーヤ 20 では、上記ステップ S 209 としてのパーソナルコンピュータ 10 からの通信に応じて、ステップ S 210 としての処理によって、フラッシュメモリ 206 に記憶されているコンテンツデータのうちから、今回チェックインされたコンテンツデータを削除する。これにより、プレーヤ 20 からパーソナルコン

ピュータ 10 へのコンテンツデータの移動が行われたことになる。つまりチェックインとしての動作が得られることになる。

【0101】6. 相互認証処理及び電源制御処理  
続いて、先に図 10 のステップ S 107 及び図 12 のステップ S 202 として示した相互認証処理について、図 13 及び図 14 のフローチャートを参照して説明する。本実施の形態としては、相互認証処理結果として認証が得られなかった場合には、USB 電源の供給制御が行われるのであるが、ここでは、この電源供給制御のための処理も含められている。また、ここではパーソナルコンピュータ 10 側とプレーヤ側の両者の処理が示されており、パーソナルコンピュータ 10 はステップ S 301 ~ S 311 の処理を実行し、プレーヤ 20 はステップ S 321 ~ S 332 (又は S 333) の処理を実行する。また、この図に示す処理として、パーソナルコンピュータ 10 側の処理は認証プログラム 338 に従って CPU 102 が実行し、プレーヤ 20 側の処理は、CPU 201 が認証処理ブロック 204 を制御することで実行される。また、認証処理結果に応じたパーソナルコンピュータ 10 における USB 電源供給制御は、電源制御プログラム 340 に従って実行する。

【0102】相互認証処理では、先ず図 13 のステップ S 301 としての処理によって、パーソナルコンピュータ 10 側において、乱数 Na を生成し、次のステップ S 302 において、パーソナルコンピュータ 10 の ID、鍵のカテゴリ番号 G、及び上記乱数 Na をプレーヤ 20 へ送信するための処理を実行する。

【0103】一方、プレーヤ 20 は、ステップ S 321 において乱数 Nb を生成し、次のステップ S 322 において、パーソナルコンピュータ 10 から送信されたパーソナルコンピュータ 10 の ID、鍵のカテゴリ番号 G、および乱数 Na を受信する。そして、次のステップ S 323 において、鍵のカテゴリ番号 G から、マスター鍵 KMa の鍵番号 j を得る。

【0104】さらに、プレーヤ 20 側では、続くステップ S 324 の処理により、j 番目のマスター鍵 KMa [j] を求め、次のステップ S 325 において、パーソナルコンピュータ 10 の ID に対して、マスター鍵 KMa [j] を基にしたハッシュ関数を適用することによって、鍵 Ka b を算出する。また、続くステップ S 326 において、乱数 Na、乱数 Nb、およびパーソナルコンピュータ 10 の ID に対して、鍵 Ka b を基にしたハッシュ関数を適用して乱数 R1 を算出する。また、次のステップ S 327 によつては乱数 Sb を生成する。

【0105】そして、次のステップ S 328 においては、これまでの処理によって得られた乱数 Na、乱数 Nb、鍵番号 j、および乱数 Sb をパーソナルコンピュータ 10 に対して送信するための制御処理を実行する。ステップ S 328 の処理の後には、プレーヤ 20 は、図 14

のステップS329の処理に進む。

【0106】パーソナルコンピュータ10では、ステップS303としての処理によって、上記ステップS328の処理によりプレーヤ20から送信されてきた乱数Na、乱数Nb、鍵番号j、および乱数Sbを受信する。この後、パーソナルコンピュータ10は、図14のステップS304に移行する。

【0107】次のステップS304においては、パーソナルコンピュータ10では、受信して取得した鍵番号jを基に、個別鍵K Iaに含まれる鍵Kabを得るための処理を実行する。また次のステップS305において、現在保持している乱数Na、乱数Nb、及びパーソナルコンピュータ10自身のIDに対して、鍵Kabを基にしたハッシュ関数を適用することで乱数R2を算出する。

【0108】そして、次のステップS306において、パーソナルコンピュータ10では、受信した乱数R1と、上記ステップS305で生成した乱数R2とが等しいか否かについて判別を行う。ここで、肯定結果が得られた場合には、相互認証の相手側であるプレーヤは、正規のプレーヤ20であるとされることになる。この場合にはステップS307以降の処理に進む。これに対して、否定結果が得られた場合には、相互認証の相手側であるプレーヤは正規のプレーヤ20として認証されないことになる。この場合にはステップS311に進む。なお、ステップS311の処理については後述する。

【0109】ステップS307においては、パーソナルコンピュータ10は、乱数Saを生成し、続くステップS308において、乱数Nbおよび乱数Naに対して、鍵Kabを基にしたハッシュ関数を適用して乱数R3を算出する。さらに、次のステップS309においては、上記乱数R3、及び乱数Saをプレーヤ20へ送信出力する。そしてステップS310において、乱数Saおよび乱数Sbに対して鍵Kabを基にしたハッシュ関数を適用して一時鍵Ksを求める。

【0110】一方、プレーヤ20側では、ステップS329の処理により、パーソナルコンピュータ10側からステップS309の処理によって送信された乱数R3及び乱数Saを受信し、次のステップS330において、乱数Nbおよび乱数Naに対して、鍵Kabを基にしたハッシュ関数を適用して乱数R4を算出する。

【0111】そして、続くステップS331においては、受信した乱数R3と、上記ステップS330で生成した乱数R4とが等しいか否かについての判定を行う。ここで、乱数R3と乱数R4とが等しくないと判定された場合には、相手側のパーソナルコンピュータ10は例えば正規のコンテンツ管理アプリケーションをインストールした機器であるとの認証を行わないことになる。そして、例えばここでは以降の処理を終了することで、例えば現在接続されている不正なパーソナルコンピュータ

10とのチェックイン、チェックアウトは行わないようにされる。これに対して、ステップS331により乱数R3と乱数R4とが等しいと判定した場合には、パーソナルコンピュータ10は正規のコンテンツ管理アプリケーションをインストールした機器である認証されたことになって、ステップS332の処理に進むようにされる。なお、ステップS331において認証を行わなかった場合には、ステップS333の処理に進むように校正することも可能ではあるが、これについては後述する。

【0112】ステップS332では、乱数Saおよび乱数Sbに対して鍵Kabを基にしたハッシュ関数を適用して一時鍵Ksを求めるようにされる。このようにして、相互認証処理が行われて双方が認証された場合には、前述もしたように、パーソナルコンピュータ10とプレーヤ20とで共通の通信用鍵である一時鍵Ksを得ることができる。

【0113】また、パーソナルコンピュータ10側での処理として、プレーヤ20を認証しなかった場合に実行されるステップS311に進み、パーソナルコンピュータ10側におけるUSB電源の供給制御のための処理を実行する。

【0114】本実施の形態としてのステップS311によるUSB電源の供給制御としては、各種考えることができる。そこで以下に、本実施の形態のシステムにおいて考えられる電源供給制御の実例のいくつかを挙げていくことにする。

【0115】1つには、ステップS311の処理として、CPU102は、例えばUSBドライバ110内のスイッチ110a（図6参照）をオフとする。つまり、Vbusを介してプレーヤ側にUSB電源を供給する動作を停止させるものである。そして、例えば以降の処理は実行しないようにされる。つまり、本来であれば相互認証処理後に行われるコンテンツデータの送受信は行われないものとされる。

【0116】このようなステップS311としての処理が実行される場合、例えば正規ではないとされる相手側のプレーヤとは、ソフトウェア的にデータ通信が行われなくなるようになるのに加え、USB電源の供給も停止されることになる。これにより、例えば単にソフトウェア的制御によってデータ通信を禁止する場合よりも強固に不正なプレーヤを排除することができ、それだけ著作権保護も強化される。

【0117】また、1つには、ステップS311において、上記と同様にして、Vbusを介してプレーヤ側にUSB電源を供給する動作を停止させた後は、図14において、破線で示すようにして、ステップS311からステップS407に戻すようにされる。つまりは、以降の処理は継続させることで、相手方のプレーヤが不正なものであったとしても、データ通信処理が可能であればこれを実行させるものである。

【0118】この場合には、例えばこの正規ではないとされるプレーヤがバッテリー駆動が可能な構成であれば、データ通信が可能とされることになる。つまり、バッテリーの残量があるうちの或る期間だけは、コンテンツデータをチェックアウトさせることなどが可能になるものである。つまりこの場合には、上記とは逆に、不正なプレーヤに対するプロテクトを緩いものとしていることで、相応にユーザに対する利便性を図っているものである。

【0119】また、次のようなUSB電源制御も考えられる。このための電源回路系の具体的構成の図示は省略するが、例えばステップS311の処理としては、USBインターフェイスのVbusを介して供給するUSB電源の電源電圧を規定よりも所定レベルにまで下げるようにするものである。例えばプレーヤ側では、チェックアウトされたコンテンツデータをフラッシュメモリ等のメディアに書き込むとき、メディアからコンテンツデータを読み出して再生するときでは、書き込みを行うときの方が多くの電力を必要とするのが一般的である。従って、上記のようにしてUSB電源として供給する電圧レベルを低下させるように制御すれば、プレーヤ側では、コンテンツデータの再生のみが行え、メディアへの書き込みは行えないようにすることが可能とされる。つまり、プレーヤ側での記録動作のみを禁止するという形態での制限動作を得ることが可能になる。このようにして本実施の形態では、USB電源供給制御の仕方によって、多様な形態による著作権保護を実現することが可能とされる。

【0120】また、例えばプレーヤ20側においても、USB電源制御を行うようにすることが可能である。つまりは、図14におけるプレーヤ20側の処理としてステップS333として示すように、ステップS331においてパーソナルコンピュータ10を正規のものであるとして認証しなかった場合には、例えばプレーヤ20側に供給されるUSB電源を内部回路に対して供給しないように制御するものである。このためには、例えば、CPU201の制御によって、レギュレータ216aの動作を停止させるなどすればよい。もしくは、上記した例に倣って、レギュレータ21から出力される電源PW・Uの電圧レベルを、再生は可能であるが記録は不可とされるまでに低下させるようにしてもよい。また、USB電源の内部回路への供給を停止させる場合には、バッテリー216を電力源とする電源PW・Bを内部回路へ供給する構成とするか否かも、例えば実際にどの程度までの著作権保護を図るのかといった事情を考慮して決定すればよい。いずれにせよ、上記のようにすれば、正規ではないパーソナルコンピュータを利用してチェックイン、チェックアウトを行おうとしているユーザに対して、制限を与えることが可能となつて、著作権保護が図られるものである。

【0121】なお、本発明としては上記実施の形態と

して示した構成に限定されるものではなく、適宜変更されて構わない。例えば実施の形態としては、パーソナルコンピュータとポータブルオーディオプレーヤとでチェックイン/チェックアウトとしてのデータ送受信を行うものとしているが、データ送受信を行う複数機器としては、これらに限定されるものではない。例えば、パーソナルコンピュータに代えて、ポータブルオーディオプレーヤとセットになった専用のEMD対応機器などとされてもよいものである。また、携帯型オーディオプレーヤ側となる機器が対応するメディアとしても内蔵フラッシュメモリに限定されるものではなく、例えば本体に挿脱可能なメモリ素子のほか、各種ディスクメディア等が採用されてもよいものである。さらには、例えばポータブルタイプに限定されず、例えば据え置き型のオーディオプレーヤとされても構わない。また、これらの機器間でデータ送受信を行うインターフェイスとしても、USBに限定されるものではなく、データと共に電源供給が可能なインターフェイスであれば本発明を適用できる。さらには、各図により示したチェックアウト処理、チェックイン処理、及び相互認証処理の実際としても、適宜変更されて構わない。

#### 【0122】

【発明の効果】以上説明したように本発明は、例えばパーソナルコンピュータと携帯型オーディオプレーヤとを、USBなどの電源供給が可能なデータインターフェイスにより接続し、オーディオデータなどの著作権が保護されるべきデータを、コピー、もしくは移動するようにして送受信すると共に、パーソナルコンピュータから携帯型オーディオプレーヤに対して電源を供給するようにされた情報送受信システムにおいて、この2つの機器間で相互認証を行うようにされる。そしてこの認証結果に応じて、データインターフェイスを介して供給される電源の制御を行うようにされる。つまり、本発明としては、認証結果に応じて電源供給を制御することで、データの送受信動作等を制限するものである。これにより、例えば認証結果に応じてソフトウェア的な処理によってのみにデータ送受信制御や機能制限制御を行う場合と比較して、或る程度の柔軟性を有したデータ送受信の制限動作を得ることができる。つまり、レベル的に多様性のある著作権保護を、電源供給制御というハードウェア的な手法によって容易に実現することが可能とされる。また、本発明としては、ハードウェア的にデータ送受信の制限を行うことになるため、例えばソフトウェア的な処理負担を軽減させることも可能となる。

#### 【図面の簡単な説明】

【図1】本発明の実施の形態としてのデータ送受信システムの構成例を示す説明図である。

【図2】本実施の形態のデータ送受信システムの利用形態を示す説明図である。

【図3】本実施の形態のデータ送受信システムにおける

チェックイン／チェックアウトの規則を説明する説明図である。

【図 4】本実施の形態のデータ送受信システムであるパーソナルコンピュータ、プレーヤの回路構成を示すブロック図である。

【図 5】パーソナルコンピュータにインストールされるコンテンツ管理アプリケーションの機能を示すブロック図である。

【図 6】パーソナルコンピュータの電源回路系の構成を示すブロック図である。

【図 7】プレーヤの電源回路系の構成を示すブロック図である。

【図 8】コンテンツデータの構造を示す説明図である。

【図 9】コンテンツデータベースの構造を示す説明図である。

【図 10】チェックアウトのための処理動作を示すフローチャートである。

\*

\* 【図 11】チェックアウトのための処理動作を示すフローチャートである。

【図 12】チェックインのための処理動作を示すフローチャートである。

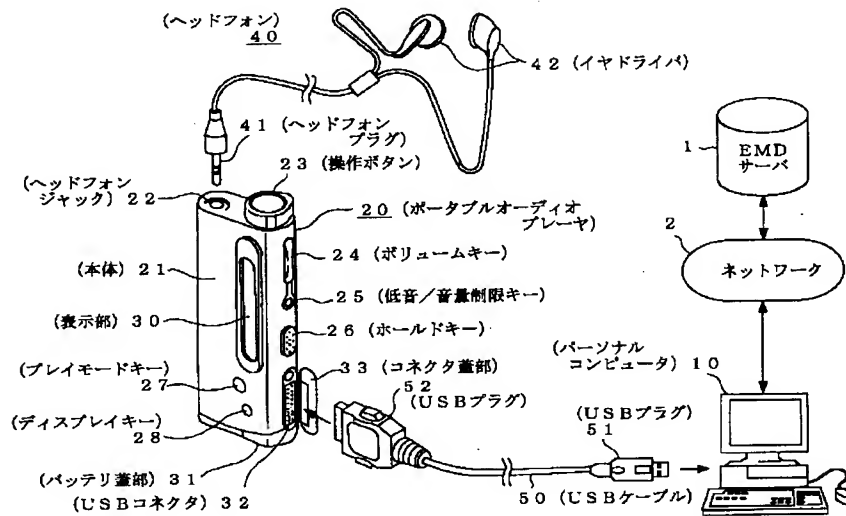
【図 13】相互認証処理を示すフローチャートである。

【図 14】相互認証処理を示すフローチャートである。

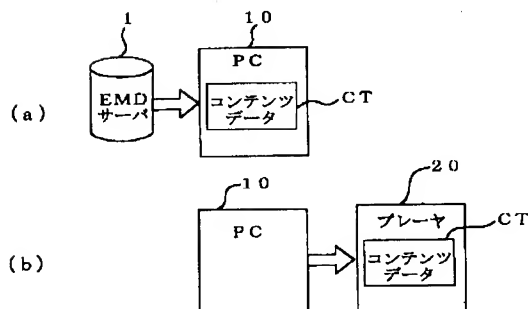
【符号の説明】

1 EMDサーバ、2 ネットワーク、10 パーソナルコンピュータ、20 ポータブルオーディオプレーヤ、32 USBコネクタ、102 CPU、107 ハードディスク、110 USBドライバ、111 USBコネクタ、114 電源部、201 CPU、204 認証処理ブロック、206 フラッシュメモリ、207 DSP、216 電源回路、217 バッテリ、314 コンテンツデータベース、338 認証プログラム、340 電源制御プログラム

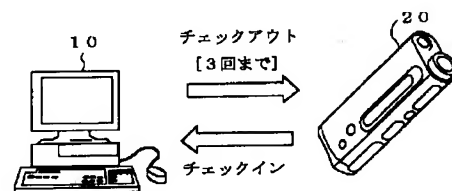
【図 1】



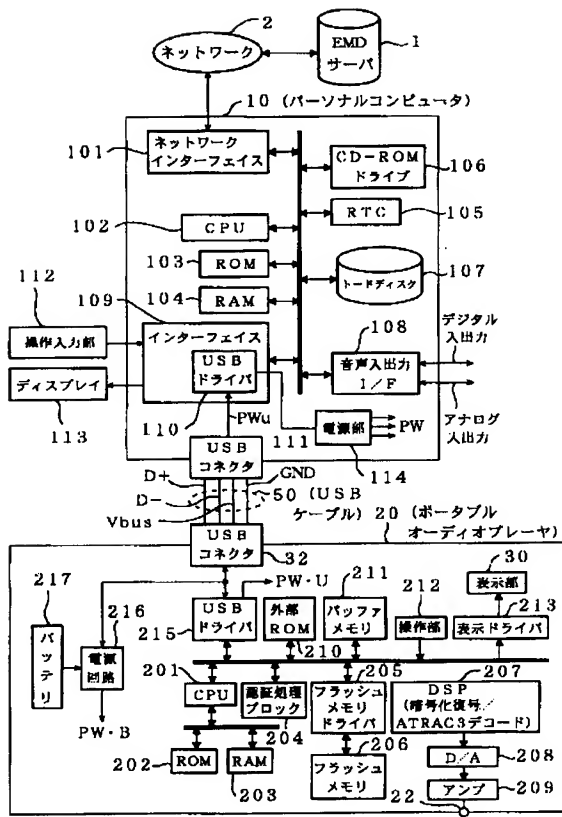
【図 2】



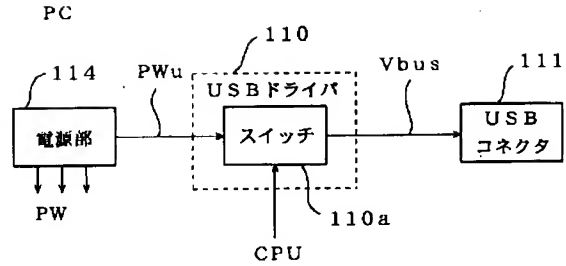
【図 3】



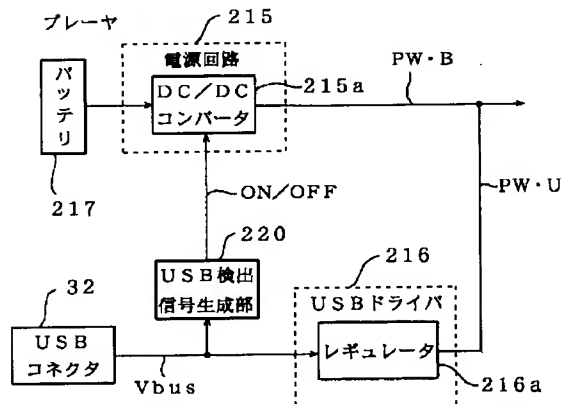
【図4】



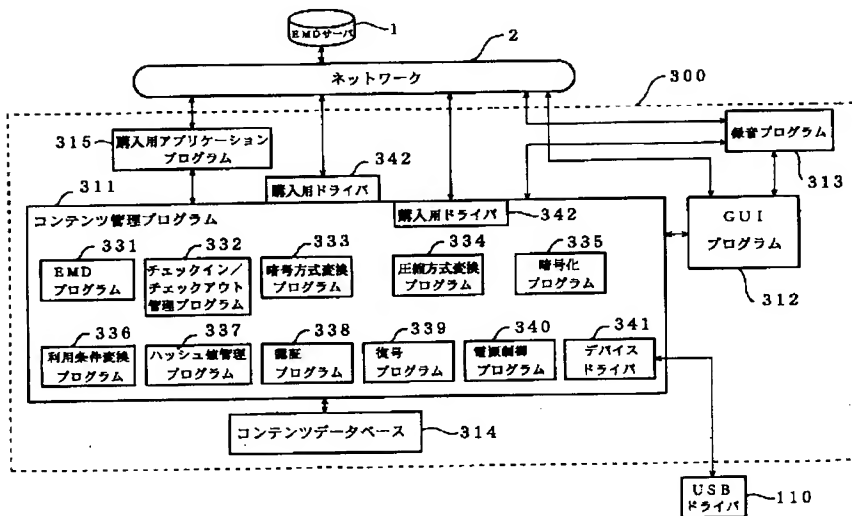
【図6】



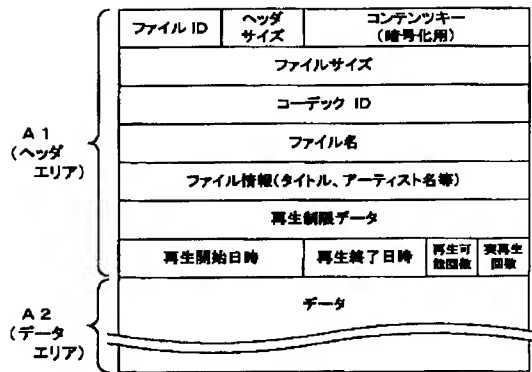
【図7】



【図5】



【図8】



【図9】

コンテンツデータベース

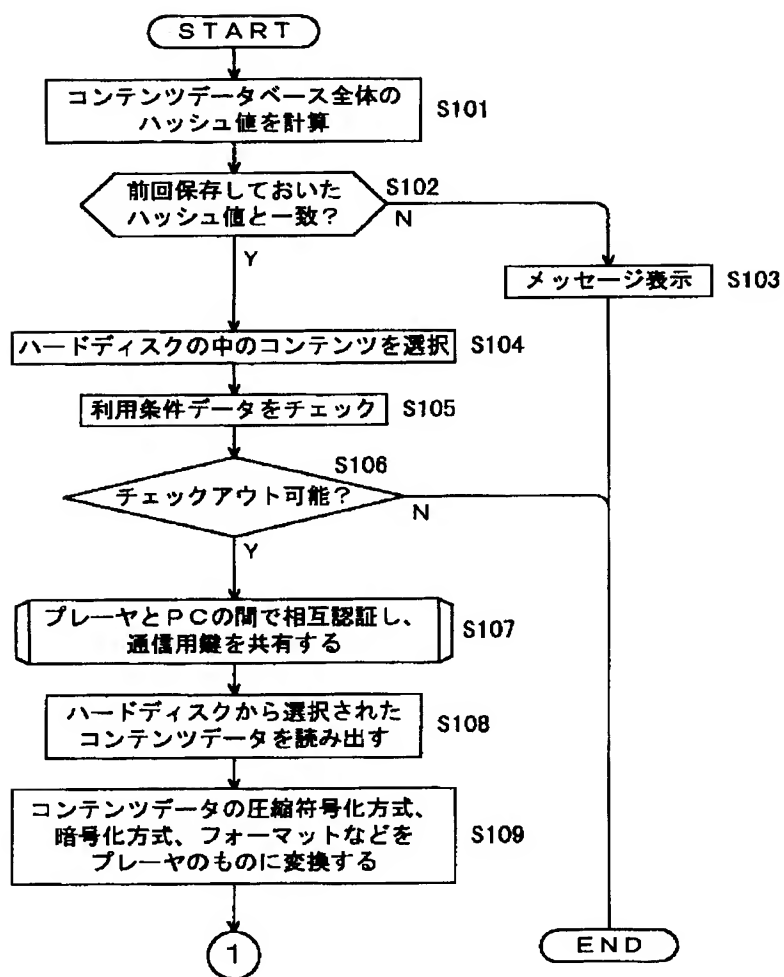
	コンテンツ1	コンテンツ2	コンテンツ3	
ファイルID	xd000110.at2	px92341234.at2	aa0234287034.at.2	
コンテンツキー	0xabababababab	0x98888888888888	0x123456789012	
タイトル	春の小川	運命	荒城の月	
ファイルサイズ	180	190	200	
再生条件:開始日時	—	2001.01.01.00:00	—	
再生条件:終了日時	1999.07.31.23:59	—	—	
再生条件:再生可能回数	—	20	—	
再生回数カウンタ	—	12	—	
再生時間条件	—	—	¥5	
コピー条件:回数	2	0	0	
コピー回数カウンタ	1	0	0	
コピー条件:SCMS	0b01	0b10	0b00	

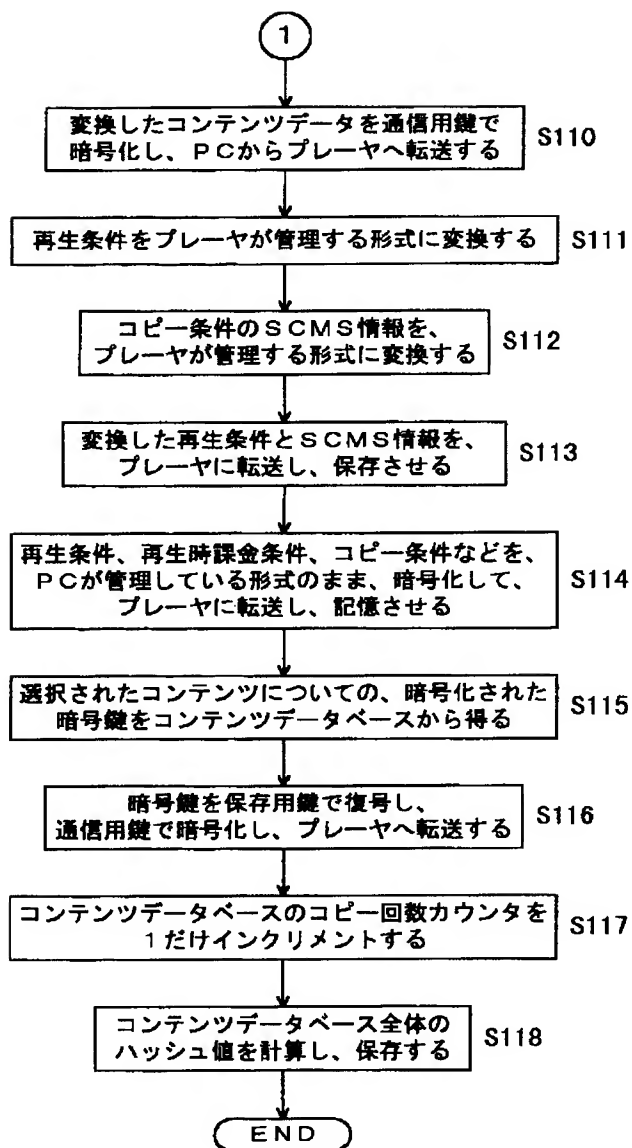
ハッシュ値	0xf9951e566321
-------	----------------

【図10】

## チェックアウト

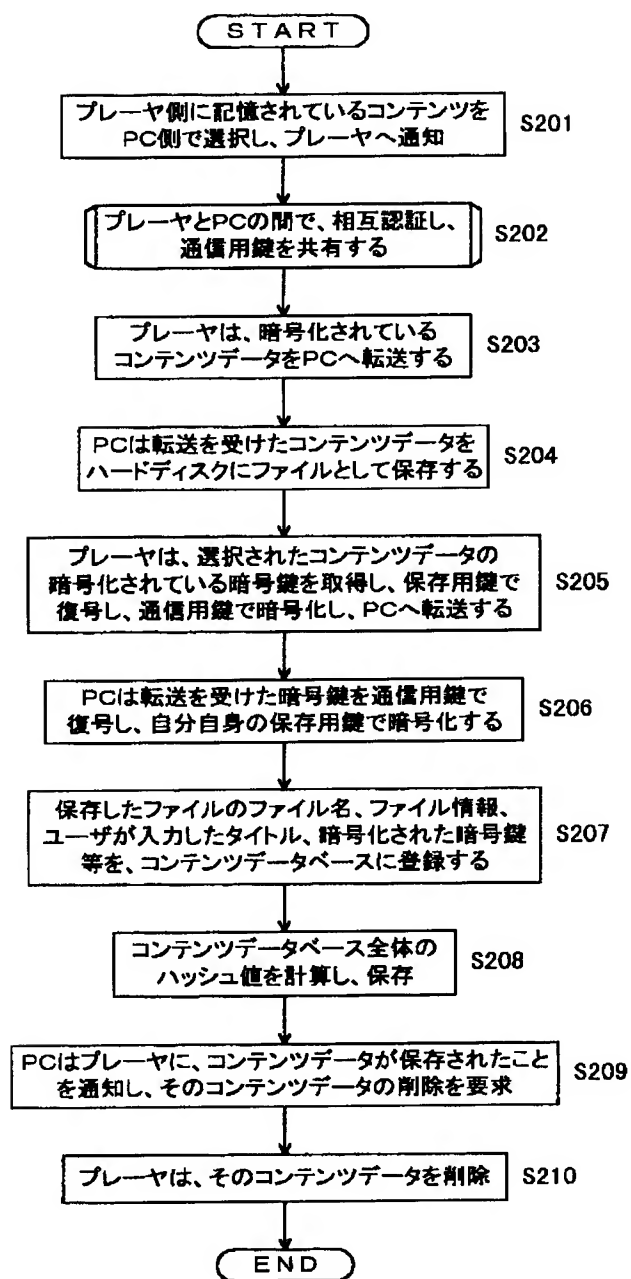


【図11】



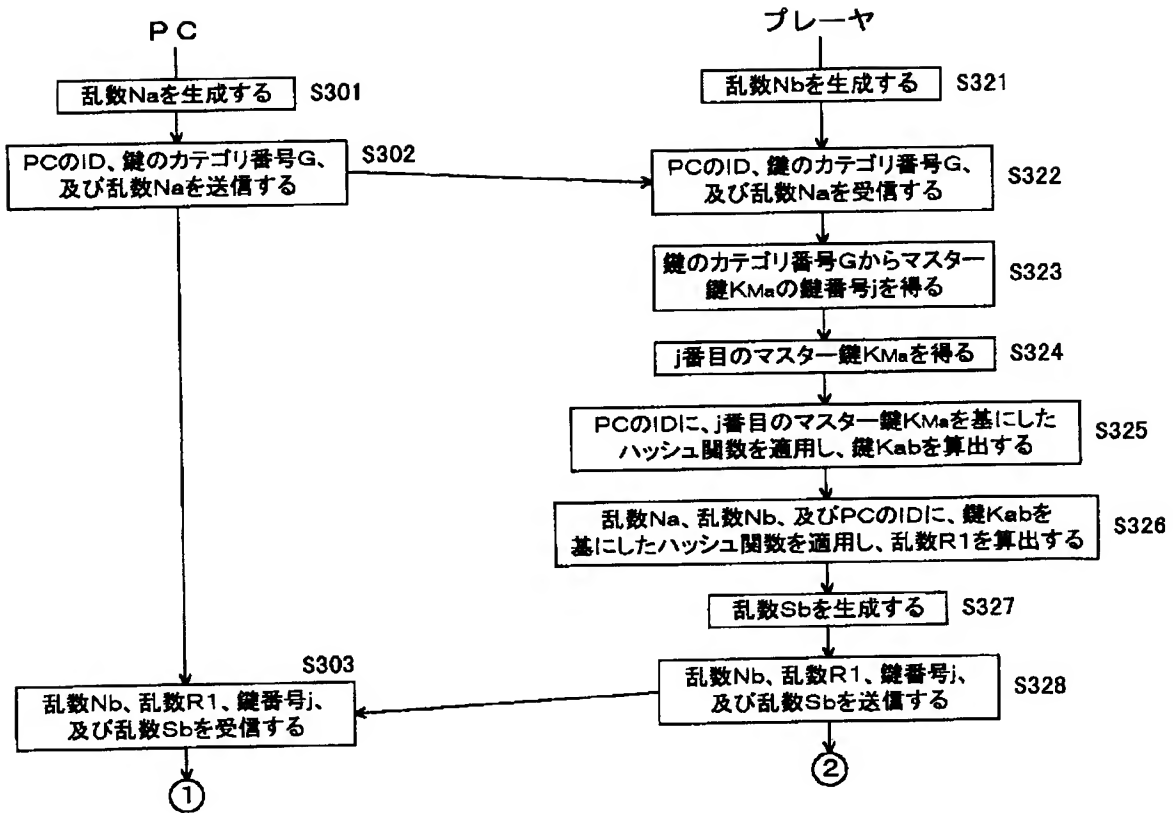
【図12】

## チェックイン



【図13】

## 認証処理



【図14】

